THE ABCs OF NFTs

BEGINNERS GUIDE TO NON-FUNGIBLE TOKENS

BARRON ROYCE

VISIT…

THE ABC’s OF NFT’s

A Beginners Guide to Non-Fungible Tokens

Table of Contents:

Chapter 1: Ethereum
Definition

- Smart Contracts
- dApps

How does it work?

- Bitcoin
- Ether

What are Ethereum's features?

- Banking accessible by everyone
- Privacy
- Peer-to-peer network
- No censorship
- Guarantee in commerce
- Compatibility

Ethereum Mining
How to store it?

- Hardware wallets
- Desktop wallets
- Mobile wallets
- Web wallets
- Paper wallets

How to buy it?

- Brokerages
- Trading platforms
- Peer-to-peer platforms
- Fintech company

ICO
How does an ICO work?
Ethereum's current ICO activity

- Golem
- EtherTweet
- Etheroll

Ethereum and ICOs
Ethereum's role in the rise of ICOs
Use cases

- Decentralized Finance (DeFi)
- Decentralized Autonomous Organizations

Chapter 2: Blockchain
What is a blockchain?
How does blockchain work?
Nodes
Mining
Is it legal?
Hash
Nonce
Consensus Algorithms

- Proof-of-Work (PoW)
- Proof-of-Stake (PoS)

Chapter 3: Non-Fungible Tokens (NFTs)
How do they work?
Owning an NFT
Creating an NFT
Rarity
Royalties
Comparing NFT network with the Internet
NFTs
Internet

Uses of NFTs
NFTs and DeFi

- NFT-backed loans
- Fractional Ownership

NFTs and Ethereum
Minting an NFT
Drawbacks

- Is it a bubble?
- Theft
- Partiality
- Environmental Damage
- Data hosting

NFT Standard
NFT Marketplaces
Is it only on Ethereum?

Chapter 4: History of NFTs
Colored Coins
Counterparty

- Spells of Genesis
- Rare Pepes

Cryptopunks
CryptoKitties
NFTs in 2020
The Rise of NFTs
Most Expensive NFTs Sold

Chapter 5: Create, Buy & Sell NFTs

- Creating an NFT
- Cost
- Selling

- Buying
- Is it a Good Idea Today?
- NFTs as an Investment

Chapter 6: Cryptocurrency

Definition

History

Why was it invented?

Ideal Characteristics

- Long-Lasting
- Divisibility
- Convenience
- Constant Value
- Intrinsic Value
- Rarity
- Acceptance

Cryptography

Chapter 7: Crypto Mining

- Verification of transaction by nodes
- Individual transaction data is entered into a list of other transactions for forming a block in the blockchain
- Along with some other data, a hash is added to an unconfirmed block
- Other miners verify it to make sure it is legit
- After it is confirmed, it gets published on the blockchain

Why would anybody mine?

Types of mining

- Cloud Mining
- CPU Mining
- GPU Mining
- ASIC Mining

Why isn’t everyone doing it?
Advantages
Disadvantage

Before we can move into our topic for today, which revolves around NFTs (Non-Fungible Tokens), we would also cover the relevant topics like Cryptocurrency, Ethereum, and others, so that you might have a better understanding of the topic. Furthermore, these relevant topics will also help you understand some vital data that will come in handy in the future.

Some topics may be familiar, but we will cover those aspects so that people who do not know much about them might benefit from that information. Not only that, but the people who also know about these aspects can get extensive knowledge or just a refresher.

For a full beginners guide on Bitcoin and Cryptocurrencies check out my other book: Bitcoin Gold: Beginners Guide To Bitcoin And Cryptocurrency (ISBN: 979-8717551847) (ASIN: B08Y5KRV94)

So, why waste time? We will dive in and obtain all the necessary information about NFTs as much as we can.

Chapter 1: Ethereum

We will start with Ethereum since it is the platform that NFT's use. In 2012, a young man named Vitalik Buterin (aged 17 at that time) learned about Bitcoin through his father. He was amused by the very concept of bitcoin and was extremely enthusiastic about its technology. He wanted to do something with Bitcoin and decided to start writing for the Bitcoin Magazine. While he was writing for the Bitcoin magazine, he suggested many improvements to the Bitcoin platform, which were ignored by the makers and managers of Bitcoin, which anyone could assume. However, instead of being disappointed over this, he decided to create a unique cryptocurrency of his own.

This disregard gave birth to the idea of Ethereum, which came to light in the year 2015. In its inception, the price of Ethereum has increased a lot. By the writing of this book, the market cap of Ethereum happens to be around $265.40 billion, while the price of Ether (ETH) was about $2,400.

Definition – So, what is Ethereum? Instead of just describing it to you in technical terminology, we will look at an interesting example.

Let there be a person named 'Jack', and Jack was a gifted rapper. Even though nobody cared about Jack's rap songs, he trusted in himself and knew that he would become a successful rapper one day. Instead of daydreaming about it, he started to get to work to achieve his goal. Now, Jack kept on writing rap songs. Jack used to write all the rap verses in an online application like Google Docs. One day, a so-called friend of Jack named John learned of this. Just like Jack is a gifted rapper, John is a talented hacker. He hacked into Jack's computer and stole all the data related to the rap songs that Jack wrote.

Knowing that he could not do anything about the lost data, Jack started to write everything again in a 'notes' app on his mobile phone. Seeing that John also hacked his mobile phone, without Jack initially knowing it, and stole his songs again. So now, Jack writes everything in a notebook with a pencil.

By seeing the example mentioned above, what are we able to make sure of? First, Jack's problem is not John; instead, his problem is that he wants something secure. Something with efficiency and convenience of writing using online apps and the secure feeling of a pencil and notebook.

What does the definition of Ethereum have to do anything about the example mentioned above? Ethereum gives you the efficiency and power of the internet, while it does not trust apps such as Google and Facebook. By doing so, your personal information would generally stay with you.

Usually, Apps such as Facebook and Google collect all your data and store that information and the information of millions of their users within their servers. This implies that the user data is kept at very few locations, which we know as centralization. Therefore, when a particular place among these locations has been hacked, the user data will be compromised.

Ethereum works so that it does not have to trust many apps with the user's private information. With the help of blockchain technology, this data is made secure in a decentralized way.

The blockchain technology used by Ethereum can be referred to as Ethereum Blockchain or Blockchain 2.0. It did not invent blockchain technology, and it makes use of the already existing blockchain technology by making some improvements to it. Ethereum uses blockchain technology more advanced compared to the blockchain technology that Bitcoin implements. The blockchain technology of Ethereum does much more than Bitcoin's blockchain, which is done in two ways.

- Smart Contracts:

The design of the Ethereum blockchain is unique, and transactions can only take place when some specific conditions have been met. The rules regarding these are known as 'smart contracts', which happen to be a vital aspect of understanding Ethereum.

For example, let us assume that a person wants to buy a soda can from a vending machine. That person is needed to put enough money into the

vending machine so that he can be able to get a soda can. If the soda can cost $2, and that person puts only $1 into the vending machine, he will not get a soda can. He will only get it if he successfully puts $2 in that machine. If the requirements have not been met, the person won't get what he wants.

Similarly, when a smart contract has been written, there is no way that anybody could do anything to change it. Hence, smart contracts can be referred to as 'Trustless Contracts'. There will not be a requirement to acquire the trust of a particular individual on the network. If the contract conditions have been met, it will happen, and otherwise, it will not.

- dApps

'dApps' or 'Decentralized Applications' are the applications that usually do not run on a traditional server. Instead, they run on a blockchain, which allows them to decentralize their server.

dApps are the central part of Ethereum's design and its views. People who founded Ethereum wanted to make sure that the users would learn about Ethereum and build on it. So, other than smart contracts, dApps are an essential aspect of Ethereum.

The coding language of Ethereum is called Solidity, which is owned by Ethereum and is used to build these dApps. Solidarity is like JavaScript, which is one of the most common languages used by developers worldwide. Therefore, developers can be able to learn it quickly and develop interesting dApps.

There is a possibility that these dApps would compete with the traditional apps and might even replace the centralized apps related to social media, e-commerce, mail, banking. Thus, the possibilities of building dApps using Ethereum's blockchain are unlimited.

So, we have learned that Ethereum is a blockchain network that allows its users to create smart contracts and dApps, which means it could forever change the internet's perspective.

How does it work? – The cryptocurrency used in the Ethereum platform is known as ‘Ether’ (ETH), and people usually get confused between these two terms. First, note that Ether is a currency, while Ethereum is a system.

To get anything done on the Ethereum system, you will need to have some Ether. Ether is responsible for the successful running of the Ethereum system, and it’s generally called ‘gas’ for this particular reason. Any transaction on Ethereum will need a specific amount of ‘gas’ to get things done. The bigger the job you want to be completed, the more gas you would require.

One of the most common that people generally ask about is the difference between Ethereum and Bitcoin. In general, people compare Ether to Bitcoin as both are the major cryptocurrencies. So, let us know more about some of the significant differences between Ether and Bitcoin.

- Bitcoin:

Bitcoin is a type of digital currency, and the blockchain of Bitcoin allows manual peer-to-peer transfers using digital money. If a person named ‘A’ wants to pay some money to a person named ‘B’ for offering services, he can do this by sending Bitcoin instead.

As we already know, Bitcoin can only exist up to a specific limit (which is 21 million). By doing so, the value of Bitcoin will increase in value like that of Gold or diamonds.

The approximate time taken for adding a confirmed block onto the blockchain would usually take around 10 minutes in general.

- Ether:

As we have already discussed, Ethereum is the network that implements smart contracts and dApps, and Ether is the digital fuel for it. For example, when the person ‘A’ wanted to send some money to person ‘B’, he can create a smart contract on Ethereum and pay Person ‘B’ in Ether. Ether is almost

like Bitcoin technology, but it comes with smart contract technology.

Here the person ‘B’ will not get paid until the job is finished, and person ‘A’ will not be able to pay person ‘B’ unless he completes the job. In real-time, this can be applied to various types of transactions, like a company paying its employees.

There is no cap on how much Ether can exist. Nonetheless, the number of Ether in existence will not exceed 100 million for a long time. This is because transactions made on Ethereum are extremely fast, which takes only a few seconds.

What are Ethereum’s features? – Let us have a look at some of the key features offered by Ethereum.

- Banking accessible by everyone:

Not everyone in the world has access to financial services, which is going to change with Ethereum. With the help of Ethereum, all you will need is an internet connection, and with just that, you can acquire lending opportunities, borrowing services, savings products, and much more.

- Privacy:

You are not necessarily required to provide all your personal information for using the Ethereum app. Ethereum wants to support the growth of value in an economy instead of surveillance over the people.

- Peer-to-peer network:

Ethereum allows you to deal with any person you want, whether making agreements, transferring money, or any relevant activities. You can cut out the middleman and deal directly with others.

- No censorship:

No specific government or a monetary authority has control over Ethereum, which means nobody can stop anyone from receiving payments or using the available services.

- Guarantees in commerce

Ethereum offers secure and guaranteed transactions, which means the money would be transferred between two parties only after everything has been done according to what was agreed by both parties. No necessity for a central authority to being able to do business.

- Compatibility:

New products and services are being launched on Ethereum daily, and these products available on Ethereum and compatible. As a result, companies can become compatible with each other and build on each other's success.

Ethereum Mining – In Ethereum, new Ether is created using a process called 'mining', which we have discussed already. The method of mining in Ethereum is like the operation of mining in Bitcoin. First, nodes present on a blockchain should verify the transactions, and then the miner nodes are rewarded with new tokens. Just like a Bitcoin miner is rewarded with Bitcoin, an Ethereum miner is rewarded with a new Ether.

We have already discussed mining in detail, and therefore, you should have a keen knowledge of what mining is and how it works. Just to be clear once again, cryptocurrency mining is like gold mining or diamond mining. Gold and diamond miners must dig, while cryptocurrency miners have to verify the transactions and add the blocks of data to the respective blockchain technology.

Just like in the process of mining Bitcoin, mining Ether makes use of a consensus algorithm called 'Proof-of-Work'. We have already discussed the PoW algorithm. However, the bad thing about PoW mining is that it uses a lot of computing power, which would result in the requirement for large amounts of electricity while making the process expensive and

disadvantageous for the environment.

Ethereum developers want to use another method called PoS (Proof-of-Stake) to resolve the requirement for a lot of energy and environmental damage. We also discussed the Proof-of-Stake method while we were discussing Proof-of-Work. This method uses significantly lesser electricity, and for that cause, it is way much better in terms of energy costs and saving the planet!

In the PoS consensus algorithm, Ethereum users having a lot of Ether with them are picked on a random basis to verify transactions. As a result, this type of mining will be rewarded with transaction fees in contrast to a new currency, and the method will require a lot less electricity, as discussed before.

People selected in the PoS for verifying transactions are known as ‘Stakers’ or ‘Stakeholders’.

How to store it? – Unlike most other types of cryptocurrencies, Ether cannot be stored outside the Ethereum blockchain, and therefore, it isn’t possible to physically store it with options. So instead, if you opt to use Ethereum, you will need a ‘wallet’, often called an Ethereum ‘address’.

This Ethereum wallet will not allow you to contain any Ether. Instead, it will enable you to acquire the codes that are needed for accessing it. Such types of codes required to include Ether are called private keys. Regardless of the reason, when you lose your private keys, you will lose your Ether. Therefore, choosing a suitable wallet is incredibly important! Just like any other cryptocurrency, there are five types of wallets available for storing these.

- Hardware wallets:

We have already discussed hardware wallets and how they can be put to use. One of the costly hardware wallets known as ‘Ledger Nano S’ offers a safe and secure way of storing the offline keys. Anyhow, just like any other set of keys (physical), a hardware wallet can be lost, and we suggest you be

extremely careful in handling it!

- Desktop wallets:

You can store your public and private keys on your personal computer with the help of a desktop wallet. This method implements the usage of a password that you should keep safe. Additionally, desktop wallets take up a lot of storage space on your system. One of the best suggestions for a desktop wallet is the ‘Exodus’ desktop wallet.

- Mobile wallets:

Mobile wallets are very much like desktop wallets; however, they use a lot of lesser space compared to the storage space used by desktop wallets. Mobile wallets are the best possible choice for storing your public and private keys on your mobile phone. ‘Jaxx’ is one of the best available mobile wallets, which offers key storage for not only Ether but 12 other types of cryptocurrencies.

- Web wallets:

You can store your public and private keys online with the help of a web wallet. One of the best available options for a web wallet is Coinbase. However, storing any sort of data online means that it is vulnerable to cyberattacks. Therefore, web wallets are considered a safe option for storing cryptocurrency of any kind. Not only that, but we strongly suggest that you should not keep vast amounts of Ether in such types of wallets, which would cause a financial loss when lost.

- Paper wallets:

We have already discussed paper wallets while we were discussing different types of cryptocurrency wallets. These are nothing but literal papers that contain your access codes written on them. Even though these types of wallets cannot be hacked, you should always be careful about where you put

them and how safely you put them.

We have already mentioned that when a wallet is connected to the internet, it would be referred to as ‘hot storage’, and when it is not connected to the internet, it’s known as ‘cold storage’. When you are storing your private keys, it is suggested that you make use of a combination of both these hot and cold wallets to get maximum security over your private keys. By now, you must have had a general idea of how you can manage Ethereum storage and choosing a wallet that is suitable for you.

How to buy it? – There are three major sources from which you can be able to acquire Ethereum, which are as follows:

- Brokerages:

Cryptocurrency brokerages are the exchanges such as ‘Coinbase’ that allow you to buy and sell Ether while charging a fee. Although being quite simple to use, brokerages can be expensive. However, with the help of brokerages, you can buy Ether using your fiat currency such as USD, GBP, EUR, and this can be done using a credit/debit card or a bank transfer.

- Trading Platforms:

Trading platforms act as a middleman between the buyers and sellers, and traders most commonly prefer these for trading cryptocurrencies. For example, using trading platforms such as ‘Cex.io’, people can trade between cryptos like selling Litecoin for Dash, buying Bitcoin with Ether.

- Peer-to-peer platforms:

With the help of these, buyers and sellers can contact each other directly and negotiate prices for buying or selling their cryptos. However, this is said to be riskier when compared to other methods for buying Ether. This is because the trading is done directly with someone you do not know. There will not be the necessity for a middleman, and hence, you won’t be required to pay any fees. Moreover, you can even pay cash as a payment method for

acquiring cryptos. One of the peer-to-peer platforms that are known as the best for purchasing Ether is ‘LocalEthereum’.

- Fintech company:

Finally, you can acquire Ether from a fintech company such as ‘Simplex’, which provides you with complete safety and liquidity while making transactions. At Simplex, you can buy Ether with fiat money, which is with the help of a credit card or a debit card.

ICO – Known as ‘Initial Coin Offering’, an ICO is to a cryptocurrency what an initial public offering (IPO) is in the stock market. Any startup company trying to raise money to create a new app, coin, or service launches an ICO.

As for IPOs, people interested in a particular startup company would invest in that company and receive shares of that respective company. When it comes to ICOs, the people who invested would be offered a crypto token, which that company has issued. This specific crypto token can be used for acquiring the services and products offered in that company. If that company does not provide any sort of such services or products, the crypto token would simply mean that the investor has a stake in the company. In general, ICOs are related to cryptocurrencies and blockchain technology.

There is a possibility that an individual might get huge profits from investing in an ICO. Yet, most of the ICOs happen to be less profitable, perform poorly, or they are just fraudulent activities. To invest in an ICO, you will need a good amount of knowledge in cryptocurrencies, crypto wallets, and cryptocurrency exchanges (which we have learned about).

A person must always be attentive while investing in ICOs because they are mostly unregulated, which means that there will be many risks involved. Therefore, you are advised to conduct research on your own about the ICO you are investing and proceed with caution. As there would be many risks involved, you should not invest aggressively in ICOs.

How does an ICO work? – when a particular cryptocurrency startup

decides to raise capital by offering an ICO, it would be required to provide a white paper consisting of the following information.

- The project description
- The products and services offered upon the completion of that respective project.
- The money needed by the cryptocurrency startup company.
- How many cryptocurrency tokens are kept by the founders of that company?
- The type of money that they will accept.
- The duration period of the ICO campaign, meaning how long the campaign would run for.

During the campaign, individuals such as supporters, fans, and other interested people would buy some crypto tokens with the help of fiat money or virtual money. These tokens offered to investors are just like what shares are to investors in IPOs.

After the campaign, if the money acquired is less than the money that the company required, that cryptocurrency startup would be deemed as an unsuccessful one, and the funds will be returned to the investors. On the other hand, if the money is greater than or equal to the required capital, it would be used by that company to acquire its goals.

Ethereum's current ICO activity – Many dApps are being created on the blockchain of Ethereum, and it implements the usage of ICOs for paying them. So, it would be beneficial to know about Ethereum's current activity.

In the Ethereum system, ICOs allow developers to market their ideas and goals so that they would be able to pay for its creation, especially for dApps.

Here are some of the dApps on Ethereum, which are being developed or already have been developed with the help of ICOs.

- Golem:

Golem is a decentralized marketplace where users can rent their system's computing power to others. Like the process of making your car available for rent when you aren't using it.

- EtherTweet:

Like Twitter, EtherTweet is a social media platform with the primary difference of being decentralized. As EtherTweet has no specific central authority, it is completely uncensored.

- Etheroll:

Etheroll is an online casino game that makes use of the Ethereum blockchain for creating dice games online. However, because of the complexity of the game and not being to understand such new types of technology might mean that your chances are not so good.

Ethereum and ICOs – During the period between 2017 and 2018, initial coin offerings (ICOs) gained popularity in the crypto community. This popular fundraising method was done by selling tokens to fund the goals and launch of a blockchain network or a dApp. Most ICOs primarily used the Ethereum network and raised a hefty sum of billions of dollars for many projects.

ICOs ultimately became a pathway to a new era of blockchain projects that significantly modified Ethereum and most crypto ecosystems. ICO's having sales of 2,000+ unique tokens gathering more than $10 billion in 2017 and 2018. Unfortunately, the ICO gold rush also became the best place for many exit scams and controversial business practices, which became the possible cause for the increase in negative attention and regulatory investigation.

Initial coin offerings, or token sales, are a unique way of fundraising and initial public offerings (IPOs). ICOs support companies in the cryptocurrency

ecosystem for raising capital and support development without the necessity of having to deal with the taxing and regulation-intensive process that is involved with traditional IPO. The tokens, which abide by the ERC-20 standard while operating in the Ethereum network, are known to promote the future of the blockchains or the specific dApps funded. Regardless of this fact, based on the nature of tokens and the process in which they were distributed, ICOs are still considered securities and are subject to regulation.

Ethereum's role in the rise of ICOs - Although most ICOs took place on the Ethereum network, the first-ever ICO known as 'Mastercoin' took place on the Bitcoin system. In the year 2013, the team of Mastercoin had a primary objective of creating a Layer-2 protocol on Bitcoin, which would issue new cryptocurrencies. This fundraising campaign lasted for a month in which any person could buy mastercoin by just transferring bitcoin to the Exodus Bitcoin address of Mastercoin. When people sent one bitcoin to this address, they would receive 100 mastercoin, along with an additional ten mastercoin every week until the sale ended. The Mastercoin sale was responsible for raising more than 5,120 bitcoins worth more than $500,000 during that period.

To most people's surprise, even Ethereum came to light with the help of a fundraising event via an ICO in the year 2014. People who wanted to have Ether would have to exchange Bitcoin for it. In the first 12 hours of sale of this fundraising campaign, approximately 7 billion Ether was sold, which was worth around $2.2 million at that time. By the time the sale came to an end, over 50 million ether was sold, approximately worth around $17.3 million. Questionably, during this time, 9.9% of ether was kept for being held by Ethereum's founding team, and additionally, another 9.9% was kept aside for the Ethereum Foundation.

With the help of Ethereum's smart contract system, developers were able to create new derivative tokens and platforms efficiently. Smart contracts were executed, automatically calculating the funds raised and distributing new tokens after completing the campaign. They would also govern the secure dynamics of the project network. As a result of this, many ICOs took place with the help of the Ethereum network, and most of them were involved with ERC-20 tokens that were immediately inter-operational with

almost all other tokens available on the Ethereum blockchain.

During the same period (between 2017 and 2018), many projects started token sales. Nonetheless, a considerable number of ICOs were not able to satisfy the requirements of the securities registration. This because most of them were very poorly created business operations, or else, they were a scam. ICOs were able to raise around $6.3 billion in the first three months of 2018, which happens to be 118% of the entire funds raised in 2017. The biggest ICO was done by ‘Block.one’, the creator of ‘EOSIO’, and raised $4 billion in 2018 alone. Another significant ICO was the social messaging app Telegram, the second largest ICO, and gathered funds of around $1.7 billion in 2018. On the other hand, the sale of ‘Telegram’ was a private sale, and only large investors were involved. Another noteworthy mention is the web browser ‘Brave’ ICO, which raised over $35 million in just 30 seconds, which is quite impressive.

Most legit blockchain projects used these raised funds from their ICOs to create and carry out successful and effective projects. But, on the contrary, it made clear that most ICOs did not possess serious teams or realistic business goals and just went with the trending hype while acquiring all the profits from beginner level to medium level investors. Due to this, ICOs gained many regulatory scrutinizes, which happened to be extremely high in the U.S. Securities and Exchange Commission (SEC).

After investigating a 2016 token sale for the DAO, the SEC provided a report that stated that the sale was considered an unregistered securities offering. In addition, a few ICO issuers attempted to evade regulations in the United States by denying access to U.S. investors on their sales.

This was not enough to stop the US-based investors as they were still able to participate in those sales with the help of virtual private networks (VPNs). And with the time, SEC took some serious action against most ICOs. This even included Block.one, which was then required to pay an amount of $24 million as a penalty. In the same way, Telegram was fined with a penalty of $18.5 million and returned $1.2 billion to the investors.

In short, people’s belief in Ethereum increased, primarily because of the popularity of ICOs. Among these ICOs, many planned for building their

products and services in addition to the Ethereum blockchain. As a result, Ethereum was able to get massive support from the community and interest from developers. The ERC-20 tokens became renowned as a widely acknowledged industry standard. Even though the interest in ICOs has been reduced to a great extent, ICOs are still happening (even nowadays). However, ICOs are taking place in a completely different manner now. For instance, platforms such as CoinList came into existence to help issuers be in accordance with Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) regulations.

Use cases – As days pass by, Ethereum is being used to create many new and unique products and services known to improve people's lives. Let us look at some of the aspects where Ethereum is being used.

- Decentralized Finance (DeFi):

An alternative to the global financial system, which provides you products and services related to banking & finance. With the help of decentralized finance, you can access services such as borrowing, saving, investing, trading, and much more on the Ethereum network.

- Decentralized Autonomous Organizations:

There are the communities owned by the members and are thought of as a safe way of dealing with strangers on the internet—considered the best possible place for committing funds for a particular cause.

Chapter 2: Blockchain

What is blockchain? – Blockchain can be understood as something like a database. It is nothing but storage for data to those who might not have heard about the term ‘Database’. For example, a computer can be called a database, as files can be stored in a computer to understand better. Similarly, the internet can also be said as a database, as it also has a vast amount of data in the form of websites, files present within it.

Usually, the data located within a database is present in electronic format, which supports our statements that computers and the internet are databases. The data present in an electronic form on a computer or the internet is present in an organized manner. The data in a database can easily be filtered by being allocated efficiently while searching for specific data. Large, complex files are stored in a database very easily. They cannot be stored in other simple things such as a spreadsheet. Unlike a traditional household computer, the devices used for databases are highly advanced computers so that a vast amount of data can be stored (of files requiring an enormous amount of storage space). Only then, these databases can work efficiently and could be used by many users a single time.

As we have already mentioned, blockchain is something like a database and not exactly one. Apart from the many similarities between the database and a blockchain, the only significant difference is that data in the blockchain is stored using bundles of data called ‘Blocks’. Furthermore, the blocks have a specific limit on how much data can be stored.

After a block in a blockchain gets completely filled with data, the data is stored in the next block. All these blocks containing the data are linked/connected in the form of a chain, and subsequently, the name ‘Blockchain’. A database, on the other hand, stores data in the form of bundles. Such as tables instead of linking all the blocks of data like a blockchain. Any blockchain is a database, but not all databases are blockchains.

Blockchains are entirely accessible by the public, making them record the transactions made, controlling the data related to those transactions, and making changes to that particular data. In each blockchain, the information can be updated independently. At the same time, all the changes made will be recorded within a master copy. Thus, the data is accessible by people located all over the world.

How does blockchain work? – now that we know what a blockchain is let us have a detailed look at its operational procedure and other aspects. To begin, we will have a look at a detailed description of the operational procedure.

- A person makes a transaction using cryptocurrency that is dependent on blockchain technology.

- The data relating to the transaction is entered into the blockchain.

- This particular data related to a specific transaction is sent to all the peer-to-peer computers in the world.

- This network of computers will now solve the relevant equations with the help of necessary methods.

- By doing so, the network of computers would make sure that the transaction is valid.

- Once the data related to a specific transaction has been validated and verified, the data will be considered legitimate.

- After being considered as legit data, that particular data related to the transactions are bundled into blocks.

- After a block gets filled with valid data related to transactions, the upcoming data will be filled into another block.

- These blocks of data would be connected to each other as if they were forming a chain.

- By the process mentioned above, a considerable amount of data

related to the transaction history is stored, which is of a vast volume and is permanent.

In this way, blockchains are created, which could store data in the form of blocks. This process does not need the involvement of governments or centralized authorities. Instead, it makes the cryptocurrency using a blockchain as a decentralized one.

Nodes – As said earlier, the data related to transactions in a blockchain are stored in the form of blocks. These blocks of data are stored on certain types of things known as ‘Nodes’. Nodes are nothing but servers, typically smaller ones. A node can be a laptop, a desktop, or even a humongous server with which the blockchain is created.

The nodes present in a blockchain are interconnected with each other. Therefore, whenever specific data has been entered in a blockchain node, it will be transferred to other nodes of that blockchain. In this way, the nodes in a blockchain will stay up to date to maintain accurate data.

Mining – The process of adding the data related to the transactions into a blockchain’s public ledger is known as ‘Mining’. Mining is the process involving a single computer being used to make all the required computations. With the help of mining, the data of the transaction history present within a blockchain is validated. After the data is validated and entered into the nodes, any attempts to double-spend the money can be stopped.

Mining is achieved by individual people known as miners. Miners solve cryptographic equations with the help of highly advanced computers. All over the world, there are countless numbers of computers involved in the process of crypto mining to make sure that the recorded transaction history on a blockchain is made secure.

When it comes to regular banks and other centralized institutions, all the information related to the transactions is managed by that same authority. This means that banks or financial institutions control, supervise, and manage the data on a centralized ledger. Every transaction made in a centralized system must go through the central monetary authority and verify and record

information. This is restricted to only a handful of financial institutions, and banks get to have their hands on the data of the central banking system.

Cryptocurrencies, as we already know, are decentralized. There is no specific monetary authority or government that oversees the data related to the transactions. Unlike a centralized system, the ledger containing the transaction history in a blockchain can be accessible by anybody. Not only that, but any individual can get into the blockchain ecosystem as a miner (a person who manages the process of mining). Transactions can be made with the help of cryptocurrencies without having to involve the central banking system.

Along with being a decentralized type of currency, cryptocurrency is also considered a distributed system. All the data related to the transaction history is made available publicly. It is stored on a vast network of individual peer-to-peer computers. This is entirely different from the aforementioned central banking system.

The central bank verifies, validates, and adds the specific data related to the transactions onto a ledger. Instead of that, the transaction-related data is added to a public ledger with the help of miners.

With the help of their sophisticated computers, Miners solve cryptographic calculations of each individual transaction and add the data related to the transactions onto a blockchain. To be rewarded for this effort, a small amount of cryptocurrency is awarded to them.

Is it legal? – In most cases, crypto mining is a legitimate and legal process that anyone can carry out. However, there might be a possibility that crypto mining might be illegal. Whether crypto mining is legal or illegal depends primarily on two factors.

1. The geographical location of the person where he or she carries out the crypto mining work.

2. The process of crypto mining, whether it is a legal procedure or is trying to mine cryptocurrencies illegally.

Using illegal means to mine cryptocurrencies, we refer to the implementation of illicit activities such as cryptojacking. Cryptojacking is the process where people (especially cybercriminals) use certain types of malware and JavaScript browsers for hijacking the processing power of other miners.

On the other hand, many countries have varied points of view when it comes to their understanding of cryptocurrencies. For example, in Germany, mining cryptocurrencies is considered a fulfilling service essential for the cryptocurrency ecosystem. On the other hand, many local governments in China regulate the mining processes of many organizations to keep the crypto mining practices in check.

Additionally, some countries even impose taxes on the income that has been obtained in the form of reward from crypto mining, while some other countries do not have such types of obligations. To have a comprehensive analysis of crypto mining, we will have a detailed look at how it works.

The crypto miners are the people who verify and validate the legitimacy of the transactions made using cryptocurrencies in a blockchain. We already know what a blockchain is and how exactly it works. The concept of blockchain involves two significant aspects, namely public key encryption and math. The blocks in a blockchain are connected, which contain the essential data along with cryptographic hashes.

Hash - Those who are not familiar with the term ‘hashe’, it is nothing but the one-way cryptographic function that makes it possible for nodes to validate the legitimacy of transactions in the process of crypto mining. A hash is the most crucial part of a block in the blockchain, present in each and every block. A hash is created by combining the header data (obtained from the previous block) and a nonce.

Nonce - A nonce is a number that can only be used once, which is a random value or non-repeating value in simple terms. During the mining process, a nonce is added to every hash in every block found by the crypto

miners.

Consensus Algorithms - A consensus algorithm such as the Bitcoin and Ethereum's PoW (Proof-of-Work) is an algorithm that requires miners to solve complex cryptographic equations (more like puzzles) for which those miners get rewarded with a small amount of the respective cryptocurrency.

People should notice that when a block is added to the network, it must follow a specific set of rules related to the consensus algorithm. For instance, some consensus rules include no double-spending, proper format of the blocks, presenting a certain amount of reward for the miners. Blocks that are not successful in following these consensus rules will be rejected. Meaning they can't become a part of the blockchain. A combination of the PoW consensus algorithm and its rules provides a robust and dependable network that is secure and makes sure that all the nodes in the blockchain validate and accept the information presented in a blockchain.

In general, consensus algorithms are composed of three major factors: security, real-time value, and fault forbearance.

- The protocol of a consensus algorithm is safe when it ensures that all the nodes that offer the exact outputs and all these outputs are validated.

- The protocol should also oversee the real-time effectiveness so that all the nodes involved with the consensus algorithm will present a value.

- A consensus protocol should finally tolerate faults meaning that it can recover when there is a failure in the operational procedure of the nodes participating in that consensus.

As there is no involvement from a central authority, the network of participants in a blockchain who develop that blockchain is required to concur on the accuracy of the information added to the public ledger of a blockchain with the help of some ground rules. A consensus must be made accessible to most of the nodes in a blockchain network. Yet, the efficiency of the implementation of a consensus is still considered work under progress.

However, the primary objective of a consensus protocol is to grant access to a node so that the nodes in a blockchain network can communicate among themselves and come up with the data accepted to be valid by all the participating nodes. Only after that, this data can be added successfully onto the public ledger of a blockchain network. In this way, miners who opt for illegal mining methods and add false data to a ledger could be kept controlled. The type of consensus algorithm varies according to the type of blockchain network. Let us look at some of the general types of consensus algorithms that are primarily used in blockchain networks.

- Proof-of-Work (PoW):

PoW is the most common and one of the most effective consensus mechanisms used for most blockchain networks. In this type of consensus algorithm, the miner will be required to solve a complex puzzle with the help of mathematics on a new block before it is validated and added to the ledger. After the puzzle has been successfully solved, the solution will be sent to other miners participating in the blockchain network and validated by them before it is accepted and added to their respective copies of the ledger. The PoW consensus algorithm also ensures that the nodes participating in a blockchain network should adopt the fork carrying the work. In almost all the cases, two competing nodes would not generate the succeeding block together.

The primary network of the blockchain offers protection against double spending with the help of verification of each individual transaction by using the PoW algorithm. In this way, the data related to the transactions are finalized and approved after the miners have done the verification. When an individual tries to duplicate a specific transaction, the transaction will not be accepted on the blockchain network as it is counterfeit. Therefore, double spending of cryptocurrencies can be stopped after the transaction has been approved.

- Proof-of-Stake (PoS):

Next to the PoW consensus algorithm, one of the most used algorithms is

PoS, which can be considered a substitute approach for PoW and requires very few requirements for mining. Even though it is also an algorithm, and the primary objective is the same as the PoW, the process is the thing that varies. As for PoW, a miner would be rewarded by resolving mathematical puzzles and creating new blocks. However, in Proof-of-Stake, the person making a new block is selected in more of a predetermined way. Based on the miner's wealth. which is referred to as stake. This means, in the PoS mechanism, there is no reward for adding blocks to the blockchain network. Therefore, the miners are paid in the form of transaction fees for their time and effort. The PoS mechanism comes with its own set of benefits and drawbacks, and the actual implementation might also be quite complex compared to the PoW mechanism.

Some other noteworthy consensus algorithms include Delegated Proof of Stake (DPoS), Byzantine Fault Tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT), SIEVE, Proof of Weight (PoW), Unique Node Lists (UNL), Proof of Burn (PoB). Implementing a specific type of consensus algorithm relies on the type of blockchain network and its relevant applications.

Comprehensive overview of crypto mining – Just so that we can understand the process of crypto mining easily, we will now have a detailed overview of crypto mining in a step-by-step manner.

- Verification of Transactions by nodes:

Transactions are a crucial aspect when it comes to the composition of a cryptocurrency blockchain network.

- Individual transaction data is entered into a list of other transactions for forming a block in the blockchain:

In crypto mining, all the transaction data is bundled into a particular list and added to a new data block. When the transaction is added to the blockchain (after successful verification of the transaction), you will not be able to double spend the fraction of bitcoin. This is done by adding the

transaction data to a permanent and public ledger. No further changes can be made to that specific data after being successfully added to a block.

- Along with some other data, a hash is added to an unconfirmed block:

After there have been enough transactions added to an unconfirmed block, some extra information is added, i.e., the header data, a hash from the previous block, and a new hash for that new block. So, what exactly happens here is that the header data of the previous block and a nonce are combined to create the new hash for the new block. Then, this new hash is added to the new unconfirmed block to be verified by a miner.

This is where you take action, and let us think that you were able to solve that. So now, you send a message to all the other miners present on the blockchain network that the mission was accomplished, and they must verify that.

How sophisticated might a hash be? Let us see an example. When you see “92a113d6d9de32e1012bc479b5225cf30850bef62b5b4855c5a436a56defb8af what exactly comes to your mind? It does not make any sense. But when we decipher it with the help of the SHA256 hash, we can see that the data is “cryptocurrency and blockchain”.

- Other miners verify it to make sure it is legit:

After you have let the other miners on the blockchain network know that you’ve successfully done it, they will have to check whether the unconfirmed block is legit by checking the node.

- After it is confirmed, it gets published on the blockchain:

Now, the PoW is complete, and it calls for a celebration when the new block of data has been confirmed. Even though the PoW consensus takes up a lot of time and effort, this is an efficient way of stating that you have solved the hash and the other miners can verify it. Since the block has been added

will be the most recent block, it is added at the end of the blockchain network. In general, all the blocks in the blockchain network are added chronologically and are added next to the previously published blocks.

The transaction data that is being added to the ledger is encrypted using public-key cryptography. To be added to the blockchain, the blocks must make use of a hash that is verified by the miner nodes on that particular blockchain. In this way, unauthorized transactions and modifications to the existing data can be prevented.

As there is no specific authority for overseeing the transactions, the computers used for mining are responsible for the ledger. Generally, the updates being made to the blockchain are frequent, and according to some research, it has been estimated that a new block of data is added every ten minutes with the help of mining when it comes to bitcoin.

Because of the blockchain, any individual can see and update the ledger as it is public. When you are a crypto miner, you will be using your computer to generate random guesses for solving the cryptographic hash. When we consider fishing, for example, if you are lucky, you will catch a fish. Otherwise, you keep on until you catch one. Similarly, if you are fortunate enough, you will be successful in solving a puzzle and get a reward, and if not, you keep going until you succeed. After trying a lot, most people would generally drop the mining process and opt for other ways of earning money.

Why would anybody mine? – We have seen that the chances of successfully solving the hash function and getting a reward for that depend on sheer luck. So, why would anybody want to go ahead and waste their precious time, effort, and money (for buying and maintaining the necessary equipment) if the chances of getting rewarded are based on luck?

There are many cryptocurrencies in existence, which most of you might not be familiar with. Most of you may have heard Bitcoin, Ethereum, Dash, but there are several thousands of cryptocurrencies in existence in real-time. By the time of writing this book, there are more than 4,500 cryptocurrencies in existence. Cryptocurrencies involve volatility, and the value of these cryptocurrencies experiences fluctuations daily.

As time passes, more and more people are attracted to making transactions online using digital money instead of standard money.

People are starting to have a little bit of doubt about the existing monetary systems. Most people would like to have control over their money and maintain discretion while managing their finances. The general ideology is that the government does not need to know what you purchase or how much you spend on your needs and necessities.

To avoid being under the surveillance of the centralized monetary authorities, some people might opt for hiding money under their basements or in an old dusty mattress in their attic (just kidding). However, there is an efficient way people can discretely use their money without involving the traditional centralized banking authorities. This can be achieved with the help of mining and making use of cryptocurrencies. Most cryptocurrencies offer a maximum level of anonymity to the people for using their money. Because of this, the implementation of the crypto mining process uses public-key encryption and hash functions.

People who mine cryptocurrencies are paid a small amount of those cryptocurrencies as a reward for their effort. This is usually a profitable aspect, yet we must consider that most people might not get the returns over the money spent by them for the resources. When a cryptocurrency is rare in nature, like bitcoin, the miners will benefit from the rewards they receive.

Cryptocurrencies are new and are gaining popularity all over the world. As a result, there has been a significant increase in the number of people who trade with them, store them, use them, and mine them.

Types of mining – As we have understood what crypto mining is, now we will see some of the types of crypto mining.

- Cloud Mining:

Cloud Mining is one of the most common ways of mining cryptocurrencies, which does not require much effort. However, it is a process where you will be required to pay a specific amount of money and

rent out their mining equipment called a ‘mining rig’, along with mining itself. In most cases, such types of mining rigs are made available by giant corporations.

This rental period would be up to a specific time that has been agreed upon by both parties. All the earnings obtained from these mining rigs would be provided to you while excluding the electricity and maintenance costs. These profits, which are generally received in the form of a cryptocurrency, would be transferred to your crypto wallet.

As mentioned above, mining facilities are offered these rigs, consisting of hundreds of mining rigs that operate together. As they are maintaining such colossal mining rigs, they have a complete idea about what they are doing, and subsequently, they are familiar with the process of mining.

Cloud mining is highly advantageous to the people who do not want to set up their mining rig or can’t afford one. Cloud mining is further classified into two different categories, which are free and paid. Generally, people tend to be attracted to the free mining process, but you should consider that it has its own set of potential drawbacks. For example, the mining speed is comparatively low, and some additional terms & conditions are involved with this.

However, paid mining is somewhat beneficial in the cloud mining process. All you must do is search for a good cloud mining host online, select one of their best plans that is suitable for you. Generally, these hosts offer 3 or 4 types of paid plans based on the features, and some might even allow you to customize your cloud mining paid plan. These sorts of plans might vary between $500 to $5,000 depending on the method chosen. Then, you must pay the amount mentioned in the plan and register your crypto wallet code with them. It is estimated that most people get the amount invested within six months to one year and profit from there. However, it would be best if you did not forget that cryptocurrencies are volatile, and nobody can anticipate a price drop.

- CPU Mining:

The name itself tells everything you need to know about this type of mining process. Processors are used in this mining process for mining cryptocurrencies, yet this is not considered beneficial.

Simple? Yes, definitely. Effective? We do not think so. Compared to other types of mining, CPU mining is extremely slow, and people might be required to wait for a longer time without having any potential returns. In most cases, people do not even get 10% of their electricity and cooling process spending. You can benefit from this process if you have meager electricity costs and excellent cooling for your processors.

So, why would anyone want to go ahead with such a mining process if it is not beneficial to them? That is because any person having a computer, especially a desktop, can start this type of mining. Yes, it can also be done on laptop computers, but laptops cannot sustain the heat, and all the circuits in a laptop would be fried in a few hours after starting the mining process. People who want to mine cryptocurrencies while not having enough knowledge on the topic proceed with this mining, do it for a few days, and stop after knowing they will not be getting money.

- GPU Mining:

The first thing that comes into mind for most people when talking about cryptocurrency mining is ‘GPU Mining’. One of the widely practiced mining processes and GPU rigs are the things that pop right into the mind while talking about cryptocurrency mining.

GPU rigs are the mining rigs that are even used in the cloud mining process as well. So, if you are doing it as an individual, it will be called GPU Mining, but if an extensive mining facility with hundreds of mining rigs does it, it would be called cloud mining.

Even though the costs involved with the construction of a GPU mining rig are costly, the efficiency of the hash speed and general workforce is excellent. Building a GPU mining from scratch would cost around $3,000, but the person will get profits much faster than he/she can get from CPU mining. A GPU rig usually consists of a processor, motherboard, cooling

system, frame, and graphic cards. Graphic cards are the essential components in the GPU mining process for mining cryptocurrencies.

- ASIC Mining:

Application-Specific Integrated Circuits (ASICs) are unique devices with an only primary objective of mining cryptocurrencies. Compared to other types of methods such as CPU Mining and GPU Mining, ASICs are highly advanced and highly effective in producing cryptocurrencies.

So, why are we even being bothered by talking about CPU Mining, GPU Mining when ASIC Mining is an extremely efficient way of mining cryptocurrencies? There is a reason for that, i.e., the controversy related to it. As ASICs are the most powerful, the chances of earning rewards with the help of GPU mining and CPU mining will become lesser. Therefore, so many miners started to protest ASIC mining to still have a chance by using GPU mining and CPU mining.

Therefore, if you choose to become a miner, it is better to opt for GPU mining or cloud mining.

Why isn't everyone doing it? - Even though there has been a considerable increase in the number of people who mine cryptocurrencies, the increase is not that large. Why is that so, and what are the reasons that people still aren't wholly getting involved in the process of mining and become miners? There are several reasons for that, and we will look at some of the significant drawbacks of cryptocurrency mining.

- As discussed, crypto mining requires a significant amount of money to start a rig because you would have to buy the equipment and manage the costs related to it, such as electricity and other maintenance costs.

- Along with that, you will need a lot of computing power to be the first person to solve the hash functions.

- The reward goes on decreasing as time goes on. For instance, if we

consider bitcoin, the compensation earned by miners used to be 50 BTC at the beginning (2009). But as of now, the reward has been reduced to 6.25 BTC. In this way, every five years, the compensation offered to miners for solving the cryptographic hash function gets reduced by half.

- Not only does the reward gets reduced, but the complexity of the cryptographic function also becomes tougher with time. This would generally result in the requirement of higher computing power, which would require more money to be put into the process to maintain the mining rig.

- Finally, some governments do not approve of their citizens getting connected with any activity related to cryptocurrencies. Therefore, if you are from such a country, then there will be a possibility that you cannot start a mining rig in your country or get involved with such activities.

- There might even be taxation on the profits earned from crypto mining depending on the geographical location you are starting a mining rig.

Having discussed that, let us have a brief yet detailed rundown on the advantages and disadvantages of crypto mining.

Advantages – First of all, we will look at the benefits of crypto mining.

- Money:

Yes, the most crucial advantage of mining cryptocurrencies is that you would be able to get money.

- Reduction in the difficulty:

We said that the complexity of solving the hash functions becomes more challenging with time. We noted that for a reason, and we will discuss it in a few moments.

However, from the end of 2018, bitcoin's mining difficulty has dropped by 15%, which is the second-largest drop in the difficulty level so far. The first significant drop being 18% in the year 2011.

The drop in the difficulty is because many bitcoin miners stopped their mining rigs after the crash of cryptocurrencies in the prior months.

When the number of miners on a blockchain experiences a decrease, the complexity of solving the hash functions also decreases with it.

We said that the difficulty level is getting increased with time, yet we again noted that there had been a drop in the difficulty level. Why is that? Let us take the blockchain network of Bitcoin, for example. Here, bitcoin's blockchain network works so that a block of data will be added to the blockchain every ten minutes on average. Which roughly leads to adding 2,016 blocks of data every week.

When the number of miners in a blockchain network decreases, the computing power is also reduced. The blockchain adjusts itself so that for every week, when there is higher computing power in use, the complexity increases, and simultaneously when the computing power is reduced, the complexity also decreases. So, if you start a mining rig when there are many mining rigs in existence, you might require higher computing power and vice versa.

- Cloud mining:

We have already discussed that cloud mining is rapidly gaining attention among people. There are two reasons for this: cost efficiency and a lesser requirement for time and effort.

When a person opts for setting up his/her mining rig, plenty of money must be spent on the hardware equipment and electricity, which could be avoided entirely with the help of cloud mining. The process for that is also straightforward. You create an account with the cloud mining host, select your requirements, and pay the amount. Simple as that.

- Resale:

If you do not like to acquire the services offered by cloud mining facilities, you can go for your individual mining rig. Meaning you would have to buy your equipment, manage the maintenance. On the bright side, even if you wanted to stop being a miner or if anything happened to cryptocurrencies all over the world, then you would still be having the equipment. This equipment can be sold again for at least the money that has been spent on acquiring it—half glass full mindset.

- Contribution:

By becoming a miner, you would be playing a significant role in the development of cryptocurrencies and becoming one of the contributing members of the cryptocurrency community. If a cryptocurrency has been accepted worldwide instead of centralized money, you will be a person that has contributed to its success. Making the world a better place for your future generations, you get what we are saying?

Disadvantages – Those are some of the advantages of cryptocurrency mining. Now, let us look at the half glass empty side, meaning the disadvantages.

- Lack of awareness:

There is no denying that cryptocurrencies happen to be highly sophisticated, and the very concept of it is still a mystery to most people in the world. “It’s rocket science! it’s quantum physics! No! it’s a cryptocurrency”. As hard as it might sound to be true, this is the fact. Most people are not even familiar with cryptocurrency (let alone its mining process).

Let us say that you are a college student and asked a thousand dollars from your friend or family member for joining the cloud mining pool. Even if trying to make them understand what you are saying, most people would still

not be interested in such types of ventures as they have truly little knowledge of the concept.

- Complex:

It is not easy to start mining as there would be a requirement for the hardware, electricity, cooling equipment, place to fix all these. So, if we have not described everything in detail, what would be your reaction when you hear the words such as GPU mining, ASIC, cloud mining pool? It would sound a bit hard to understand these aspects, right?

Even after knowing about all these aspects, you would still need a lot of time and effort and no need to say money.

- Costs:

First, you would need to buy hardware such as processors if you are willing to set up an individual mining rig. For that, you need money. Now, this equipment will not run on its own, right? You need electricity for that. Again. Money! So, these processors and other hardware must work very efficiently to solve a complex hash function, and such types of equipment get heated quickly. To cool these, you will need equipment related to cooling, and what will you need again? Exactly!

Moreover, if you do not have your place to set up a mining rig, you would have to rent it. You are using hardware equipment, which means that you will be facing technical issues and other relevant problems every now and then. To rectify such issues, you know what is necessary. You can see where we are going with this.

- Increase in the difficulty:

We already discussed that reducing the number of miners on a blockchain network would reduce the difficulty level. Similarly, when there is an increase in the number of miner nodes present in a blockchain network, there will be an increased difficulty level.

- Illegal Activities:

People who opt for cloud mining companies are usually at the risk of being vulnerable to a scam. Many fake companies and illegal organizers want to make you pay the subscription plan amount along with your mined coins while you remain with a bit of amount, which is not all a reasonable thing for your efforts. If you want to go with cloud mining, it is suggested that you do some ground research and make sure that you choose a renowned company with good feedback from the public.

- Possibility of loss:

We are being optimistic and stating that you would generally get rewards from your mining process after a certain period. However, you should not take it for granted because there is a possibility that you might even lose the money. If we look at the last few years, we have learned that cryptocurrency prices are highly volatile. Therefore, there is a possibility of prices going down drastically while affecting the mining rig's profits. Also, based on the costs related to the hardware, electricity, and cooling, a decrease in the prices could mean that you are spending more money on the mining rig when compared to the cryptocurrency you are receiving back in tokens. Therefore, using an ASIC miner can be highly beneficial, yet you might have to be on the lookout for the downsides of using an ASIC miner, as we have discussed before.

Chapter 3: Non-Fungible Tokens (NFTs):

Another important use case of Ethereum is a Non-Fungible Token (NFT). Most of you may have been familiar with the fact how popular NFTs have become these days. So, what is an NFT?

NFT – To understand what a Non-Fungible Token means, let us have a look at the name itself. Non-Fungible means something unique, more like one of a kind, which cannot be replaced with something similar to that, and 'Token' refers to an 'asset' or a 'unit'. So, combining the words, Non-Fungible Token is a unit or an asset that is genuine, unique, and cannot be replaced, representing the ownership of something of greater value. With the help of these non-fungible tokens, things like art, digital collectibles, and much more.

To make it more straightforward for you, let us see an example of this. Fungible assets are things that can be traded for another of the same kind. For example, a Bitcoin is a fungible asset, and you can get another Bitcoin by exchanging this Bitcoin. Any Bitcoins will have the same properties. On the other hand, things such as the Kohinoor Diamond or the Mona Lisa Painting are only one of their kind. You cannot get another one similar to those by just exchanging it, or you cannot make an identical copy of it.

NFTs are designed in such a way that they can only be under single ownership at any given time. These are made secure with the help of technology related to Ethereum's blockchain. Any person cannot change the ownership of an NFT into their name or create another copy of that. Most NFTs belong to real-world items such as artwork or real estate.

How do they work? – In general, almost all the NFTs exist in Ethereum, yet other blockchains can make something like these using their technology (some already did).

Some of the exquisite features of NFTs are as follows:

- There is a unique identifier for each and every token that has been

minted.

- NFTs cannot be interchanged with other tokens of the same properties. So, if we see an example, One Ether has the same value as another Ether, but one NFT will not be the same as another NFT.

- There is an owner for every token available, and information regarding this can be easily verified.

- They exist on the Ethereum network only, and any person can buy or sell these NFTs with the help of an Ethereum-based NFT market. (we will discuss some of the best marketplaces available for NFTs in a while).

Owning an NFT - When you own an NFT, it is easy to prove that you are the genuine owner of that NFT. Once you own an NFT, there is nothing anyone can do to manipulate it. You can sell an NFT that you own, and you can even earn royalties on the resale if you created that. If you do not wish to sell an NFT under your ownership, then you can keep it with you forever in a secure way by storing it in a wallet.

Creating an NFT - When you make an NFT, you can prove that you are the actual creator. You would be the only person who can determine the rarity of that NFT. Let us say that you created an NFT of digital art, and you sold it to someone else, and that person sold it to another person. Now, when that happens, as you are the creator of the NFT, you will receive royalties. These royalties are not provided just once; instead, they will be provided to you every time there is a resale. You can be able to sell your NFT on any NFT marketplace or in person. There is no specific requirement for the transfer to be done in a particular platform only. On the bright side, you will not even be needing anybody to act as a middleman for selling your NFT.

Rarity – As we discussed earlier, the rarity/scarcity of an asset is determined by the creator while dealing with NFTs. For instance, think that there are tickets being sold for a concert. Let us assume that you are the organizer of that event. Now, you can choose how many tickets are needed to be sold. If we believe that you are a creator of NFT here, you are the only person that can decide how many replicas of an asset should exist. There can

be exact replicas of a single asset, which means you can determine the number of the same type of seats, let's say 500 standard tickets. Here, all the 500 tickets are of the same value, which means they are the replicas of a single unit.

Sometimes creators can make NFTs that are minted in a remarkably similar manner, yet they are slightly different from each other. For example, there are 500 tickets for 500 seats, but each seat ticket with a different seat number.

The creator can also create an NFT, where only one NFT will be minted as a unique type of asset. For example, as an organizer, you will be printing unique barcodes on the tickets, which are only accessible to the person intended for having them. This means there would be only one owner for each NFT, making them unique.

The scarcity of NFTs is entirely dependent on the intentions of the creator. A creator can make an NFT wholly unique with only one minted, or he or she can opt for having many replicas. However, one should never forget that the information related to the scarcity of an NFT is public, which means you cannot sell them to two different people saying they are the only ones minted.

Royalties – In some cases, NFTs will automatically pay royalties to their respective creators when a sale occurs. Even though this process is still being developed, it happens to be very efficient. For example, the original owners of 'EulerBeats Originals' tend to earn a royalty of 8% every time there is a sale of that NFT. Platforms such as 'Foundation', 'Zora' support the concept of paying out royalties to the artists using their platform.

The process of royalties being paid is entirely automatic, which means that the creators can relax. At the same time, they earn royalties on their work whenever sold from one person to another. At present, knowing about the royalties is a manual process, and therefore, it is not so efficient or accurate. As a result, most of the creators are not being paid what they deserve. However, when an NFT contains a program for earning royalty, the creator would never miss out on the royalties when a resale happens.

Comparing NFT network with the Internet – With the help of NFTs and Ethereum, many problems that exist on the internet are being solved nowadays. With time being passed, almost everything is becoming digital. It is essential to use the features related to physical things like rarity, uniqueness, proof of ownership. As we all know, digital items usually work according to the context of their specific product. To state an example for this, let us look at a few things you cannot do.

- Imagine that you have purchased a movie or a game on the Play Store. You cannot re-sell those to somebody else.

- Suppose you have earned some reward points or loyalty points from a particular website. You cannot exchange those loyalty points for getting rewards or credit on any other platform, even if the things you have are extremely popular and people want to have them very badly.

The internet is not as beneficial as the network/internet of NFTs is. Here is why:

NFTs:

- NFTs are entirely unique, and there is not a possibility for any two NFTs being the same.

- Every NFT has an owner, which is established on a public record so that anyone can easily verify it.

- NFTs, in general, is compatible with any platform that has been built with the help of Ethereum. For instance, an NFT autograph can be traded on any Ethereum marketplace for acquiring an utterly different NFT, such as a rare collectible!

- Creators of NFTs can sell their work anywhere in the world and can have access to a worldwide market.

- Creators can let go of their ownership rights on a specific NFT they own and continue to have royalties from the resale of those assets.

Internet:

- On the other hand, people can get a copy of a song or any other file, precisely the same as the original file itself.

- Organizations manage the information related to the ownership of a particular item. They are stored with the help of their servers. So, if you want to verify that information, it might be a bit hard for you.

- Companies on the internet, which offer digital items, must build their own platform. For example, an app that offers digital tickets should have its own ticket exchange as well.

- Creators can only sell with the help of the platforms they own. There might be certain types of terms and conditions on the geographical locations they want to sell.

- Platforms like music streaming services offer profits to singers, which mainly occur from the sales.

Uses of NFTs – Some of the fields in NFTs are used Digital Content, Gaming, Domain names, Physical assets, Financial aspects.

One of the most common uses of NFTs at present is many aspects related to digital content. A significant cause for that is the poor performance of the digital industry, where most of the profits and earning potential of content creators are taken away by platforms.

If we consider the artists on social media, when an artist posts content on a social network, the platform gets more profits as it shows ads to the followers of that artist. Some people get a small amount of money for doing so, while some others get exposure. But the company gets more from the businesses whose ads are being published. The exposure is not enough for an artist to deal with the financial aspects of his/her life.

With the help of NFTs, a new economy is being made for the creators, where those creators will not give their content to the platforms for free so that they can make money by showing ads. Ownership is connected to the

content itself.

When a creator opts to sell their content, the funds are directly presented to them. If there is a resale of that content, the original creator will receive royalties automatically. This is going to happen every time it's sold. Why? Because the creator's information is embedded into the token's metadata, which is impossible to modify.

There has been much enthusiasm over NFTs, especially from game developers all over the world. This is because NFTs usually provide ownership data-related items in games, boost the performance of gaming ecosystems, and come with a wide range of benefits for the players.

In most games, people can buy items to use to get ahead in the game faster. If that person wishes not to play that game anymore, all the money that has been spent on the game would be in vain. However, if the items you buy in the game are NFTs, you could get back all the money spent by you by just selling those items when you do not want to play the game anymore. There might even be a possibility of gaining profits if the item has good demand by the time, you sell it.

In any particular game, the game developers would be considered creators of that game. Hence, when they create an item, they could earn a royalty every time there is a resale. This opens a gateway to an advantageous business model for both players and developers, as they can gain from the secondary NFT market.

Cryptocurrency addresses come with a combination of various numbers and alphabets, which is hard to memorize. For example, when a person asks you for your Ethereum wallet address, you can remember something having 64 characters and looks like ‘bj2xbi4HalnsFl22qJ…’. Therefore, NFTs make it easy for you to modify your Ethereum address with something you can remember, such as ‘myethwallet.eth’. Thus, you can easily remember your Ethereum address and easily tell it to other people in such away.

This is known as ‘Ethereum Name Service (ENS)’, which is just like a domain name service used as an easy way to remember an IP address. Like domains, ENS names also have some value based on their length and

relevance. With the help of ENS, you will not be needing a domain registry for dealing with the process of ownership transfer. Instead of that, you can just trade your ENS names using an NFT marketplace, which is way easier.

The ENS name will allow you to receive cryptocurrency tokens and other NFTs. In addition, you will be pointed to a decentralized website, and you can also store some of the vital information such as profile info, email addresses, Twitter info.

The tokenization of physical assets has not been developed as much as the tokenization of digital assets. Therefore, many projects concentrate on creating ways to tokenize real estate, rare fashion items.

We can see that NFTs are very similar to deeds. There might come a day when buying automobiles, or a house can also be done using NFTs. If such things were to happen, the NFTs will have the ownership information, while the payments could be made with the help of Ether.

When such a time comes, and physical assets would become (somehow) accessible on the Ethereum network, then you can put those as collateral for obtaining a decentralized loan on Ethereum.

NFTs and DeFi – Both the ecosystems of NFT and DeFi (Decentralized Finance) have been collaborating in many ways, which are as follows:

- NFT-backed loans:

There is an availability of some DeFi apps that allow you to borrow money by providing collateral. For instance, when a person wants one bitcoin, he or she would be required to provide 25 ETH or 26 ETH as collateral. A person can get the loan he needs, and if the borrower defaults the loan, then the lender can get the collateral. But not everyone would have the required amount of cryptocurrency with them for acquiring the loan they need.

To help such people, there have been some upcoming projects, which are starting to find out the methods for using NFTs as collateral. For example,

imagine you bought a rare NFT a few days ago, which is worth, let us say, $63,000 based on today's prices. By keeping this as collateral, you can secure a loan of 26 ETH. If you cannot pay back the ETH, your rare NFT will be sent over to the lender as collateral. This could work for anything that can be tokenized as an NFT.

This will not be a complex process as both the DeFi and NFT worlds use Ethereum’s blockchain technology.

- Fractional Ownership:

Creators are also able to create ‘shares’ for their particular NFT. This allows investors and fans to own an NFT by just owning a part of it and without having to buy the entire asset. With the help of this, more and more opportunities are becoming accessible to the minters and collectors of NFTs.

Such types of fractions of NFTs would be traded with the help of Decentralized Exchanges (DEXs) such as Uniswap and not just the NFT marketplace. By doing so, there would be a significant increase in the number of buyers and sellers.

The overall price of an NFT can be determined with the help of its fractions. You will be having a window for owning and gaining profits from the items that mean a lot to you. It would be excruciating when you wanted to have something, but you cannot pay that much.

To make it simple for you, this would be something like owning a piece of a Picasso. You would have a stake in a Picasso NFT, which means you also become a part-owner and have control in involving things like revenue sharing. It's possible that soon enough, owning a part of an NFT will allow you to enter into a decentralized autonomous organization (DAO) to manage that particular asset.

DAOs are the institutions powered by Ethereum and allow anonymous people, such as worldwide shareholders of an asset, to harmonize securely without trusting the remaining people. Even a single cent cannot be spent without the approval from all the members present in a group.

As we've said before, the space of NFTs, DAOs, fractional tokens are all under development at different paces. Nevertheless, all their infrastructure can exist and work together as they all belong in the same network, i.e., Ethereum.

NFTs and Ethereum – Ethereum makes it possible for NFTs to run smoothly depending on many aspects, some have been given below:

- The transaction history and the metadata related to tokens are public, and anyone can verify these. Therefore, it is straightforward to prove ownership with the help of NFTs.

- After successfully confirming a transaction, it is impossible to manipulate the existing data, which means the ownership status cannot be stolen.

- Trades in NFTs could be made directly, which means there will not be a necessity for platforms that usually take a part of the money as compensation.

- The products available on Ethereum implement the same type of technology. Therefore, even if you have an NFT in one platform, you can sell it on another platform as long as it is Ethereum.

- Creators can simultaneously list multiple properties, and all those products would still have the up-to-date information available.

- Ethereum is available 24/7, which means you can sell your NFTs whenever you want.

Minting an NFT – To mint an NFT, the following things are done.

- The NFT should be confirmed as an asset existing on the blockchain.

- The account balance of the creator should be updated so that the asset will be included. By doing so, it can be made sure that the person owns that asset.

- The transactions mentioned above are to be confirmed and added to a

block on the blockchain while making it permanent (immortalized).

- It should be confirmed by people in the network to be valid so that it would be accepted that the NFT is on the network and it belongs to the creator.

- As it exists on the public ledger, anyone can be able to check it. Finally, this would result in an increased earning potential of the creators.

The tasks that have been mentioned above are usually done with the help of miners. Miners let other people on the network know about these NFTs and the person who owns them. The process needs to be difficult, or else any person can claim the NFT with the help of fraudulent ownership. To make miners work honestly, there are many incentives.

While the blocks of data are being added to the blockchain of Ethereum, they need to be created consistently. So, for every 12 seconds, there will be a block of data added to the blockchain. However, nobody could alter this data, which is being added to the blockchain. For example, when a hacker tries to modify the data of an NFT in a block, let us say block #200. When he tries to do that, the data on the other blocks will change, and when it happens, any miner on the Ethereum blockchain might identify it and stop it from happening.

Both NFT transactions and everyday transactions are added to the blockchain alike, which means a block with no NFT transactions would be the same as the block with NFT transactions. This means that the computing power needed is also the same. Therefore, the environmental damage is done because of the blockchain or Ethereum rather than being done because of NFTs.

Drawbacks – We have covered most of the features and advantages of NFTs, and some things are impressive about it. However, there are some drawbacks of NFTs, which are given below:

- Is it a bubble?

There is a possibility that, like most other lucrative cryptocurrencies, Ethereum is also subject to specific scrutiny. If all the countries come together and decide to ban cryptos and everything associated with it, then you would say goodbye to all your valuable NFTs. So, it is a unknown for the future to have cryptocurrencies in implementation.

Countries like Bolivia, China, Algeria, Morocco have banned cryptocurrencies and any relevant activities. Additionally, countries like India are trying to impose a ban on cryptocurrencies, and things are in the process of doing so.

So, when something is too good to be true, it is, and the same might apply to cryptocurrencies and NFTs as well.

- Theft:

Suppose a person worked extremely hard and produced digital art. Before he could mint it as an NFT, some other person can steal it by hacking and make it his own NFT. There is no specific regulation for preventing such types of activities.

- Partiality:

People who are famous and gained a reputation might get a huge fan base and make a lot of money, whether from selling songs, art, or anything else. So, what about the upcoming artists that are trying to gain an audience? They probably cannot make much money because most people prefer buying something from somebody famous. So, it might be that favorable to upcoming artists and creators who are in the beginning stage of their careers.

- Environmental Damage:

The most crucial disadvantage of NFTs is that it runs on Ethereum, and Ethereum needs mining for the blocks of data to be added to its blockchain. This is not only for Ethereum, but it is the same for most cryptos, especially ‘Bitcoin’. Opting for mining with a Proof-of-Work (PoW) consensus

algorithm would require a vast amount of computing power. There would be a need for highly advanced computers and much electricity. It was estimated that the energy used for the mining activity of Bitcoin was more than that of the energy usage of entire Argentina. This would result in environmental damage, and the carbon emissions could be drastic.

After Bitcoin, NFTs gained a lot of hype and popularity, and there would be an increase in the activities related to these. So, there is a possible chance for NFTs to become the second most significant factor of carbon emissions and environmental damage considering all the cryptos in the cryptocurrency ecosystem.

- Data Hosting:

The digital asset and NFT are stored individually, which means the NFT is located on the blockchain while containing the information where the digital asset associated with it has been found. The digital asset is usually connected to an NFT with the help of a link. If the digital asset has been deleted from the place where it has been stored, or the server that hosts the NFT faces any technical difficulties, the link would no longer operate efficiently. As a result, the NFT will become worthless. There is no possible way to back up the NFT if any such situation occurs.

However, as it was mentioned before, Ethereum is planning on switching to Proof-of-Stake (PoS) instead of Proof-of-Work (PoW). By doing so, they can reduce the environmental damage to a great extent as there will not the necessity for highly advanced computers or a considerable amount of electricity.

NFT standard – Token standards are the set of rules or code that allows for easy integration across a wide range of platforms on the network, compatibility with other platforms on the network, and an increase in the utilization of the value and the network effect. The token standard for NFTs on Ethereum is ERC-721.

The ERC-721 (Ethereum’s request for comments) comes with a standard for NFT. For example, stating something like ‘this Token is unique and has a

different value than another Token from the same Smart Contract, which can be because of its age, scarcity or even something else like its visual.'

NFTs contain a unit256 variable known as a 'tokenId', which must be unique for every ERC-721 contract (along with the contact address). This tokenId could be used as an input in a converter, which would get outputs such as weapons in games, kittens in cryptokitties game.

While the token standard, namely ERC-721, is only used for NFTs, ERC-1155 can be used for both the fungible and non-fungible assets on a smart contract.

NFT Marketplaces – NFT marketplaces are the platforms built with the help of Ethereum, which allows people to buy, sell, or create NFTs. NFTs are available to everyone, and not just only for the rich people. So, let us have a look at some of the best available NFT marketplaces that would come in handy for you if you needed to involve with NFTs.

- OpenSea
- Superfarm
- Rarible
- Ethernity
- Enjin
- FansForever
- Hoard.Exchange

These marketplaces have been described as some of the best where you can get involved with NFTs.

Is it only on Ethereum? – So far, almost all NFTs are present on the network of Ethereum, yet other blockchains can create something like NFTs using their own blockchain technology.

Cryptokitties, which allows people to buy virtual kittens, want to switch to FLOW blockchain from the Ethereum blockchain, which uses PoS consensus and supports NFTs.

Tezos is another blockchain system that also runs on the PoS consensus and allows the sale of NFT artwork.

Chapter 4: History of NFTs:

Colored coins – According to most people, Colored coins that existed between 2012 to 2013 are arguably the first types of NFTs. Colored Coins comprised of smaller denominations of Bitcoin.

These could even be a single Satoshi, which is the smallest unit of Bitcoin and is equal to 0.00000001 BTC (1 Bitcoin = 100,000,000,000,000 satoshis). Colored Coins could represent various types of assets and many use cases, which are as follows.

- Property
- Coupons
- Subscriptions
- Digital Collectibles
- Issuing own cryptos
- Issuing company shares

Colored coins were responsible for massive growth in the opportunities of Bitcoin. One of the drawbacks of these colored coins was that they only represented specific values, only when everybody agrees on their worth. The scripting language of Bitcoin was never meant to support these types of things on its network, which made colored coins become the weakest part of Bitcoin.

For instance, if five people agreed that 1000 colored coins were used to represent the shares of a particular company, and even one person disagreed that they can’t be used to express that company’s shares, then the total concept is invalid.

The drawbacks of colored coins were evident because the Bitcoin network worked in a permissioned system, and it was better to use it as a database. Nevertheless, colored coins created a gateway for other inventions of NFTs.

Counterparty – After colored coins, many people believed in the

possibilities of issuing assets on blockchain networks. Most people also agreed that Bitcoin's network was not meant to support these types of features. In 2014, people named Robert Dermody, Adam Krellenstein, and Evan Wagner introduced something called a Counterparty.

This was a peer-to-peer financial platform with a distributed protocol built with open-source internet on Bitcoin's blockchain network. Counterparty granted access to the creation of assets on a decentralized exchange along with a crypto token of its own, namely XCP. In addition, several projects were comprised of a trading card game, meme trading.

- Spells of Genesis:

People who were the creators of the game 'Spells of Genesis' were the first who successfully issued in-game assets on a blockchain with the help of Counterparty. Not only that, but they also happen to be the first-ever to launch an ICO. The name of ICOs did not even call ICOs, and people referred to them as 'crowdfunding' or 'fundraising' during that time. The developmental activity of Spells of Genesis was funded with the help of a token called 'BitCrystal', and these BitCrystals were used to buy things in their game.

- Rare Pepes:

Can you even imagine memes as a part of the blockchain? Yes! Memes! You have heard it right. After games were a part of blockchain technology, people thought, 'why don't we add memes on a blockchain?'. This led to the issuing of 'Rare Pepes' in October 2016, which were used as assets on the Counterparty platform.

During that time, the fanbase of memes was proliferating. Additionally, there was a meme exchange known as 'Rare Pepe Meme Directory'. The uniqueness doesn't stop at being present on a blockchain, and the Rare Pepe Meme Directory also consisted of 'experts' who certified the rarity of Pepe memes. Nowadays, Counterparty has various types of projects that are like NFTs.

As Ethereum started to gain popularity, memes started getting traded on Ethereum's network. In 2017, a project started on Ethereum with 'Peperium', a decentralized marketplace for memes and a trading card game that allowed individuals to create memes that would exist permanently. Like Counterparty, Peperium also had its token called 'RARE', which can develop memes and listing fees.

Cryptopunks – Since Rare Pepes was able to pick up the pace on Ethereum, two technologists came up with an innovative NFT project. John Watkinson and Matt Hall wanted to create unique characters that were generated on the Ethereum blockchain. They set a limit for the characters to exist, which is 10,000, and no two characters would look the same. These projects started with its name as 'Cryptopunks'.

After the project started, the creators of Cryptopunks let anyone claim a Cryptopunk for free. Not literally anyone, but anyone with an Ethereum wallet. After all these 10,000 characters were declared, a secondary marketplace emerged, where people would buy and sell these.

There was no ERC721 token standard in implementation because it has not been invented yet. By that time, ERC20 was in existence, and Cryptopunks did not even follow that standard as well. However, they did follow the ERC20 standard, but only up to a certain extent.

CryptoKitties – NFTs came into light with CryptoKitties, as it was the game that made NFTs famous. As the name itself suggests, this is a virtual game with cats on a blockchain, where a person would have to adopt, raise, and trade virtual cats.

This project had many booms on many news media such as CoinDesk, CNN, and many more. But unfortunately, it was also one of the factors responsible for the lagging of Ethereum because people had a craze for these on the blockchain. To most people's astonishment, some of the kitties were sold for a price of around $100,000. Yes, you have heard it right. But who would buy virtual cats for such hefty sums of money? Well, people with much money are interested in virtual cats compared to real cats.

CryptoKitties was launched by a Vancouver-based company called

‘Axion Zen’ in the year 2017. The alpha version of CryptoKitties was launched at the ETH Waterloo Hackathon. The developers were working on the project for a few months before that. ETH Waterloo Hackathon was the best place for the launch of CryptoKitties as it was the world’s largest hackathon conducted for the Ethereum ecosystem. CryptoKitties came in first place in the hackathon, which led to a rapid rise in the popularity of this game.

In the same year, the crypto market was very efficient, which CryptoKitties get more attention from people worldwide. This created an interest for NFTs among the people. Axiom Zen started a company called Dapper Labs, which obtained $15 million in funding. Even certain corporate investors such as a16Z and Google Ventures also invested some funds into this. Through all this, people started recognizing the true potential of NFTs and started paying more attention to them.

NFTs in 2020 – There was a considerable response towards NFTs during 2018 and 2019. Many projects started taking place, and by the year 2020, this popularity was increased to a great extent than before. One of the major factors responsible for this is the accessibility of NFTs, which was quite easy to be accessed by beginners. With the increase in marketplaces and Web3 wallets, NFTs will have a promising future, depending on blockchain technology.

Web3 wallets are the self-custodial wallets through which an individual will be provided with the entire ownership, and he/she would be solely responsible for their assets. Web3 wallets come with all the necessary regular functions along with a dApp browser so that they can be able to access decentralized applications.

On the other hand, smart contract wallets are online programs on a blockchain that present a public key and private key to the user.

The Rise of NFTs – In 2021, we have seen much development in the cryptocurrency ecosystem and the industry of digital assets. This has been one of the most essential and contributing factors for the rise of NFTs.

So far, digital artwork worth $208 million was sold on the NFT markets,

which includes secondary sales as well. This is good progress compared to the overall $250 million worth of digital artwork that was sold in 2020.

We can also see that Bitcoin has reached over $63,000 in April 2021, which happens to be the all-time best of Bitcoin's price over its entire history. By considering these factors, we can understand that cryptos and NFTs have gained popularity. Additionally, people are interested in letting the public known about EFTs with the help of social media platforms such as YouTube, Facebook, and Podcasts.

They are also proven to be highly advantageous for the creators and investors, as discussed before. Creators gain much exposure, and the ownership data cannot be modified. The creators are also entitled to royalties, which means they can earn more and more money every time there is a resale. Let us see an example.

A person named Ryan Maloney, a digital artist created a series of cards called 'Beastly Ballers'. While he was making these, Ryan only thought of printing these out and sell them for $4.99 for every ten cards. However, Ryan changed his thoughts on this as he heard about the evolution of digital assets and the concept of NFTs. Afterward, Ryan listed these collectibles on an NFT marketplace and was able to sell 14 cards for a price of $700 (one card being sold at $85).

By looking at this scenario, we can understand how creators can get the actual worth for their artwork.

Most expensive NFTs sold – Some NFTs were sold for millions of dollars while some were sold for a few bucks. We will now look at the details of NFTs that were sold at a remarkably high price compared to other NFTs.

1. **Everydays: The First 5000 Days**

The most expensive NFT so far was the 'Everydays: The First 5000 Days', which also happens to be the most expensive artworks sold. This was created by Mike 'Beeple' Winklemann, a collage containing 5,000 artworks of Beeple, which represented his artistic skills during his career.

This was sold for an amount of $69.3 million at an auction conducted by Christie's, and the first time in history where an auction house sold a digital artwork.

It was purchased by a person called 'Vignesh Sundaresan' (CEO of Portkey Technologies) with a pseudonym as 'MetaKovan'. Initially, Vignesh disagreed on revealing his identity, but he revealed it afterward. He said that the main reason for this was to show the world that even Indians and other people of color can also contribute towards crypto technology, just like the rest of the world.

During this auction, the second-highest bid was made by Justin Sun, who was the CEO and founder of Tron, and the bid amount was a hefty $60.2 million, which was the highest bid until Sundaresan came over.

2. Cryptopunks (#3100 and #7804)

Both Cryptopunk #3100 and Cryptopunk #7804 were for an amount of 4,200 ETH. However, there is a price difference between these two NFTs. How can there be a difference in the price if both were sold at 4,200 ETH? Cryptopunk #7804 was sold on March 10, 2021, and Cryptopunk #3100 was sold on March 11, 2021. As we all know, the price of Ether is volatile and increased by a few thousand dollars on March 11. Therefore, Cryptopunk #3100 was sold at a higher price equivalent to $7,584,485, while Cryptopunk #7804 was sold at a price equivalent to $7,566,173.

Cryptopunk 3100 is a blue-colored alien type Cryptopunk containing a band with the colors white and blue. On the other hand, the Cryptopunk 7804 is also a blue-colored alien type Cryptopunk, which can be seen wearing glasses and a hat while smoking pipe.

3. CROSSROAD

CROSSROAD is an NFT that Beeple also created. It consists of an image containing an individual (Donald Trump) lying down with some words related to 'defeat' written all over the body. This artwork was created in

correlation to the 2020 election and its outcome. If Trump won, there would be an artwork containing Trump wearing a crown and walking through fire.

One of the popular NFT marketplaces that is a platform for most digital collectibles, known as Nifty Gateway, was responsible for selling this artwork. Sold by a Twitter user named ‘Pablorfraile’ for $6.66 million and was bought by an unknown person. The seller initially purchased it four months before this transaction, and it was estimated that the sale fetched him ten times profit on the actual amount spent for buying it.

4. The First Tweet

An NFT was created for the first-ever tweet of the cofounder and CEO of Twitter, Jack Dorsey. This was not only the first tweet made by him, but it is also the first tweet that was made on Twitter. The auction was conducted throughout March in 2021 and was sold for a price of $2.9 million finally. This NFT was minted with the help of a platform known as Valuables, which lets users create NFTs and represent their Tweets. Jack Dorsey, who happens to be a philanthropist, converted the entire funds to Bitcoin and donated all of that to Africa Response.

5. Cryptopunk #6965

After the alien-type Cryptopunks, the next rarest type was the ape Cryptopunks. Cryptopunk #6965 is an ape type Cryptopunk with a ‘Whatever’ type of expression. This was sold for an amount of $1.54 million in February 2021. The details regarding the seller and buyer for this NFT are unknown. Recently (during the time of writing this book), this NFT has been listed for sale again for around 2,100 ETH. Equivalent to $50.5 million. If this NFT is successfully sold, the seller would be sitting on a massive pile of money.

6. Genesis Estate

This is a piece of land (virtual land) on the gaming platform Axie Infinity

and was sold for 888.25 ETH, which was equivalent to $1.5 million during that time. On February 28, 2021, this transaction was sold by Axie Infinity to a new player on the platform, namely ‘Flying Falcon’.

7. Auction Winner Picks Name

This is an NFT, which is as peculiar as it sounds. An American DJ named ‘3LAU’ created a music video and dance track in collaboration with a digital collage artist named ‘Slimesunday’. This music video was created and auctioned on Nifty Gateway to let the buyers name it (whatever they want). So, the buyer will not only get to choose the name of the NFT and other open editions and get the first edition of the available editions worth $9999. It was sold for an amount of $1.33 million, while the buyer's details remain anonymous.

8. Cryptopunk #4156

Another Cryptopunk NFT sold for a colossal amount was Cryptopunk #4156, which was sold for around $1.3 million. This Cryptopunk was just like Cryptopunk #6965 (ape type), with almost everything similar except Cryptopunk #4156 has a blue bandana. This transaction took place in a public auction, while buyer and seller details remain anonymous.

9. Not Forgotten, But Gone

This was an NFT that consisted of artwork created by a famous artist called ‘WhIsBe’, renowned for creating gummy bear murals all over Brooklyn and giant statues existing in public places (in many parts of the world). Over the recent days, WhIsBe became familiar with the concept of NFTs and opted for showing his talent in the world of NFTs.

As a part of this idea, he created a 16-second video that consisted of a gummy bear skeleton known as ‘Not Forgotten, But Gone’, which was the most expensive NFTs created by him and was sold for an amount of $1 million on the NFT marketplace Nifty Gateway’.

10. The Best I Could Do

‘Justin Roiland’, the co-creator of the animated television series called ‘Rick and Morty’, is famous for his abilities in productions and voice-overs. Justin also happens to maintain an animation studio as well as a video game studio. In January 2021, Justin decided to sell a collection of his artwork with the implementation of blockchain technology. On January 18th, Justin raised more than $1 million for his artwork with the help of NFT marketplace Nifty Gateway. This collection of his artwork was called ‘The Best I Could Do’, which was even tweeted by Justin.

Chapter 5: Create, Buy, and Sell NFTs

So far, we have learned about the definition, the working procedure, and other important aspects of NFTs. Most of you might wonder how we can create NFTs or buy/sell them. Let us discuss how we can create NFTs, buy them, and sell them.

Creating an NFT – Creating an NFT artwork, regardless of whether it is a GIF, image, or anything else, is a straightforward process and doesn't require any extensive knowledge regarding the cryptocurrency ecosystem or the blockchain network. However, we have provided everything in this book so that you might refer to the content, with whatever you might be unfamiliar with.

You can even choose the blockchain on which you are trying to create your NFT. However, there are not many options available for creating NFTs (regarding their blockchains), and Ethereum is the most efficient way, if not the only way of getting involved with NFTs.

Coming to the other blockchains that allow the operations of NFTs, each type of blockchain has its way of dealing with NFTs. For instance, if you opt for the Binance Smart Chain blockchain, you would only be able to deal with NFTs by using the assets of Binance Smart Chain only. This means you will not be able to create, buy or sell NFTs that belong to some other type of blockchain on the Binance Smart Chain blockchain network. Therefore, it is highly suggested that you choose the Ethereum blockchain because it is the most popular type of blockchain for dealing with NFTs.

To create your own NFTs with the help of the Ethereum blockchain, you would be required to have some of the prerequisites and necessities.

- You would need an Ethereum wallet, which would support the token standard if ERC-721. Some of the best Ethereum wallets available in the market, which abide by the ERC-721 standard and deal with NFTs, are 'MetaMask', 'Trust Wallet', 'Coinbase Wallet'.

- Minimum balance of Ether, which can equivalent to $50 to $100. While using wallets such as Coinbase Wallet, you might be able to buy Ether with the help of their platform using various types of currencies such as USD, GBP, and many other fiat currencies. However, if you go for any different kind of wallet, you might have to buy Ether with the help of any other cryptocurrency exchange.

After you acquire a wallet, the next thing required to concentrate on is the NFT platforms that will allow you to connect your wallet with that platform and upload the digital asset, which you would like to change into an NFT.

We have already discussed the NFT marketplaces, which happen to be the best in the market. Marketplaces are not only the platforms that allow you to buy or sell the NFTs, but they also allow you to create your own NFTs. However, you would be required to register with that specific marketplace and become an artist on their platform.

Some NFT marketplaces such as Rarible, OpenSea, and MIntable have a button named ‘Create’, which usually exists on the top right corner of their platform. So, for instance, let us consider the medium of OpenSea to understand the scenario better.

A ‘create’ button will allow you to access a screen, which will require you to connect with a wallet based on the Ethereum blockchain. After entering the username and password, you will automatically be connected to the marketplace. However, you might also be required to sign a message digitally so that you can be able to prove that the wallet details you have entered belong to you. This process of verifying your ownership over your wallet would not require any sort of fees or charges.

The next step is to go to the ‘create’ button and select the ‘my collections’ option from there. By completing this step, you will be able to see the ‘create’ button. On clicking that, a window will pop up on the screen, which would allow you to upload your artwork (digital asset), add a name for it, and enter the description. This process creates a place where you can create a folder where you can store the NFTs you want to create. After you have successfully created an image or any other asset into your collection, you will be able to see it. Upon completing that, you can also create a banner image by

clicking on a ‘pencil’ icon that appears in the right corner.

Once this process is complete, you will be allowed to create your very first NFT. Now, clock on the ‘add new item’ option, upon which you will be required to sign another message. Now, you will be redirected to a window where you can upload the NFT image, audio, GIF, or any other type of digital asset.

In most platforms like OpenSea, you will be presented with options that will allow you to add some unique characteristics and attributes to increase the rarity and the uniqueness of the digital asset. There is even an option, which enables users to add some information that any other person cannot unlock except the person who purchases them. This content can be passwords or any other specific services that would allow access to discount codes or contact details. After finishing that, you must click on ‘create,’ requiring a final signature to create your NFT. Congrats, now you can see your artwork appear in your collection.

The cost involved with creating – Some platforms such as Open Sea will charge nothing to make an NFT, while some other marketplaces might charge fees. Most of the marketplaces based on Ethereum will refer to this aspect as gas, which has been discussed earlier while talking about Ether. This gas is the amount required for carrying out certain types of functions. While we are talking about creating NFTs, the gas would be needed to create NFTs onto a marketplace. The costs regarding Ether would vary based on the network and based on the specific type of marketplace, and the costs can be high.

Helpful tip – If you want to make a transaction using Ether, the costs might be considerably cheaper during the weekends when compared to the weekdays. The main reason for that is the lesser number of transactions that are carried out during the weekends. When the transactions are few, the significant costs related to making transactions with Ether. Suppose you are willing to list multiple NFTs at a particular time.

Selling NFTs – We now know how to convert our digital assets into NFTs. Now, we will look at the process of selling those NFTs. To sell your NFTs, first, you would have to locate your NFTs in your collection. After

discovering them, you would be required to click on them and then click on the ‘sell’ option. By selecting the sell option, you will be redirected to a pricing page to determine and create the terms and conditions of your sale. This includes the options of whether you would like to set an auction for them or sell them for a specific price.

Ether and certain other types of ERC-20 tokens are the available cryptocurrencies for you to sell your NFTs. However, most platforms would only allow their native cryptocurrency to be able to make transactions. For instance, when you look at the VIV3 marketplace that runs on the blockchain technology of FLOW blockchain, the only cryptocurrency tokens with which you will be able to make transactions are the FLOW tokens and the FLOW tokens only.

In the OpenSea marketplace, there is an ‘edit’ button located right next to the collection. By signing the message using your wallet and scrolling down a bit, you will see some options regarding the royalties and the token you would like to receive to sell your NFTs. Royalties, as we know, have the possibility of earning passive income for a lifetime whenever there is a sale of that respective assets. The process of royalties is successfully sustained with the help of smart contracts (thanks to Ethereum).

In some cases, you might be charged a fee for listing your NFTs on a marketplace. Therefore, even though it is not the case for all the NFT marketplaces, it is better to deal with such situations.

Buying NFTs – Before hastily purchasing NFTs, some factors are to be taken into careful consideration. We will now know about these crucial factors, which are particularly important while purchasing NFTs.

- The marketplace you want to choose for buying NFTs.
- The wallet you will be needing for getting connected with the platform where the NFTs are being sold.
- The tokens (cryptocurrency) you need for funding the wallet and buying those NFTs.

- It is knowing whether the NFTs you want to buy are being sold at a particular time, which is through a pack or an art drop.

According to the aspects we discussed while we were talking about the expensive NFTs sold so far, we can see that some NFTs could only be sold on specific platforms only, such as Nifty Gateway, Rarible. So, to make it easy to understand, let us know an example covering this aspect.

If you want to buy an NBA Top Shot pack, you will need access to an account with NBA Top Shop, a Dapper wallet, and the ability to fund it with USDC Stablecoin or any other fiat currencies that support it. Unfortunately, this will not suffice because you would also have to wait for a specific period until there is an announcement for the drop of a particular pack of the card to try to buy them before they are sold out (depends on your luck).

This method of Pack drops/art drops has been gaining popularity because it is the most efficient way for selling rare and unique NFTs to the people who are eagerly waiting for them. It is better to register and fund your wallet before itself so that you will not miss out on the opportunity of buying them, as the sale might be completed within a few seconds after its starts. Keeping everything ready might save time.

Is it a good idea to buy NFTs now? – The NFT boom has just started and based on what we have to say; it may continue. Also, many celebrities, such as Shawn Mendez and Grimes (Elon Musk’s child's mother), are opting for NFTs to sell their digital assets such as music or artwork. Based on this, NFTs would experience more popularity compared to what we are currently seeing now. Furthermore, as more blockchains are competing to provide services related to NFTs, now is a good time as any for buying NFTs.

NFTs as an investment – even though there is some acceptance towards NFTs worldwide, NFTs are still considered a new type of investment. Moreover, it is tough to determine the value of a digital asset, which makes NFTs a risky investment option.

When it comes to stocks, the possibility of an increase in the price is higher, which certainly means that you would be able to sell it for a higher price even after ten years, if not now. That is not the case with NFTs because

NFTs are artwork, and there is no certainty for an increase in their price. You cannot be able to determine whether a meme, or a gif, or any other digital asset to experience a hike in their price.

Regardless of what was said above, most of you would still see NFTs as a lucrative form of investment. If so, make sure that you have a specific limit on how much you spend on them. Along with that, you should also make sure that your investment portfolio's risk tolerance is enough to deal with a loss that occurred because of investing in NFTs (if any loss were to happen). Also, remember that NFTs are highly speculative, which means you cannot entirely rely on them for becoming rich.

Even though NFTs can be considered a good form of investment, they are not considered ideal for everyone, and not every digital asset is an ideal NFT. If you have a substantial amount of money, which you can afford to lose, you might try your luck in NFTs. However, if that is not the case, then it is better to avoid getting involved with NFTs so that you can keep your hard-earned money safe.

Chapter 6: Cryptocurrency

Definition – A cryptocurrency is a currency present in a digital form, which does not have a physical presence at all. Cryptocurrencies make use of the cryptography method secure from being double-spent and work based on blockchain technology.

In simple terminology, a cryptocurrency is a type of digital money dependent on a network called blockchain, distributed across many computers and maintains a public ledger of all the information. Blockchain technology is a decentralized system, which means that they exist so that the governments and central authorities are not involved with them.

The term ‘cryptocurrency’ is broken into ‘crypto’ and ‘currency’, which means encrypted money based on encryption techniques used to secure the network. Blockchains, which we have discussed already, is the organizational methods for ensuring that the transactional history is valid and is the crucial component of most cryptocurrencies.

According to the experts in the banking and finance sector, it is believed that blockchain and the technology related to it will create many hassles in various industries, including finance and law.

However, Cryptocurrencies are being criticized for various reasons, such as their use for illegal activities, volatility, and the network's vulnerabilities. Nonetheless, they have been appreciated for their portability, divisibility, resistance to inflation, transparency, among many other aspects.

Cryptocurrencies are the type of money that grants access to make secure payments online, which are present in virtual ‘tokens’ (literally meaning that they don’t exist) represented with the ledger entries made internally into the network. Here, ‘Crypto’ points out the various encryption methods and cryptographic techniques that oversee such ledger entries, including elliptical curve encryption, public-private key pairs, hashing functions.

Cryptocurrencies like Bitcoin are not physical money, yet they have

strived to become a financial breakthrough. Here is your comprehensive overview for understanding cryptocurrency and all other relevant aspects. If you are thinking about knowing whether it's the right time to become a part of the cryptocurrency market? That is good, and most people are thinking of doing the same. If you want to go with crypto mining and earn money, you can refer to the information mentioned earlier in this e-book. However, some other methods help you make money with the help of cryptocurrencies, which we will discuss below. Not only that, but the information that we are about to provide will be helpful to you in knowing extensively about cryptocurrencies.

The financial journey of cryptocurrency owners (especially when it comes to some specific ones such as Bitcoin) has been volatile since the beginning. Looking at Bitcoin, we can see that It started as a typical worthless investment, yet it went on and became an asset with a price of $64,500 by the time of writing this e-book. This price has seen many ups and downs, and by downs, we mean drastic drops that would make any investor panic.

There are even some banks that are interested in the application of blockchain technology in their business activities. Yet, cryptocurrencies such as Bitcoin were developed so that people can avoid the use of banks altogether. Developers of cryptocurrencies and their fan communities like the ideology of a decentralized network that will not require any other parties to process a transaction. Even with a centralized network, a bank would still be a third-party that wants to access the information and is not anywhere near cryptocurrency. Therefore, Crypto owners usually tend to go with their money.

History – How did it start? To answer that, we might have to look at the past as far as 1983. During that year, an American cryptographer named ‘David Chaum’ came out with an idea for cryptographic electronic money known by the name of ecash, which was known for maintaining its anonymity. After some time passed by, in 1995, he implemented his idea through Digicash, the first type of electronic payment. This makes the use of cryptography and requires user software to make payments in a similar way that we usually withdraw notes from a bank and designate specific encrypted

keys before that very payment can be sent to another recipient. This feature allows digital currency to be anonymous and untraceable by a bank, the government, monetary authority, or any third party, for that matter.

In 1996, a paper was published by the National Security Agency, namely 'How to Make a Mint: The Cryptography of Anonymous Electronic Cash', which describes the procedure and working of a Cryptocurrency system, which was first published in an MIT mailing list. Later in the year 1997, it was also published in 'The American Law Review'.

After that, in 1998, Wei Dai published an illustration of 'b-money', which is distinguished as an anonymous, allowed electronic cash system. Within a short time after that, Nick Szabo stated it as bit gold. Like bitcoin and other cryptocurrencies that would follow it, bit gold was described as an electronic currency system. It required users to complete a consensus algorithm (Proof of Work) function with cryptographically put solutions together and published. People should confuse it with BitGold, which is a gold-based exchange that came into existence later.

However, the first decentralized cryptocurrency that came into existence was Bitcoin, which was created in 2009, presumably by a person or a group of people known by the pseudonym developer Satoshi Nakamoto. It made use of SHA-256, a cryptographic hash function, and implemented a proof-of-work consensus protocol. We will discuss more on Bitcoin in a few more moments. In April 2011, a cryptocurrency named Namecoin, which happens to be the first attempt at creating a decentralized DNS (Domain Name System), made internet censorship to become quite difficult. Within a short time after that, Litecoin was released in October 2011. Instead of making use of SHA-256, it uses scrypt as a hash function.

Why was it invented? – What was the actual reason that a person had to go and invent some digital currency such as a cryptocurrency? Why wasn't everyone happy with the paper currency most used by the people of the nations in the world?

Paper currency was not the first currency that people have used to purchase things or make transactions. First, the evolution of money went from seashells, wheat bags, and other not-so-traditional forms of money.

Then, people started using things that are more valuable and could be easily stored or managed.

To understand the evolution process of money, we might have to look at some of the characteristics of money, making it the best to use.

As we all know, money is used to maintain some value to be exchanged to get other objects. This was the primary objective of money when there were no other obligations, such as transactions and forex trading.

When a person wants to buy bread or gas or anything else, he or she might have to pay money (of the equivalent value) in exchange for those objects. Here, the person compensates the seller of those objects with cash in exchange for what they acquired. In this manner, money keeps revolving from one person to another while helping them gain the things they want.

As discussed before, paper currency was not available, and people opted for a wide variety of things. However, back in the early ages, a system in implementation known as the ‘Barter System’ roughly translates to an exchange system.

Here is a brief description of how the barter system works. Suppose there were two people, where one person had a wheat bag, and the other person had some fruits and veggies. Then, the first person wanted to have what the second person had and vice versa. Now, they just exchange the things they have in between them, which results in mutual satisfaction. It sounds like a good system. Well, we are coming to that part.

When the barter system was in effect and a few centuries after that, the most common types of things that people used for money are stones, seashells, wheat, salt, and gold.

Ideal Characteristics - Money would be considered ideal when it has some characteristics, which we will discuss below.

- Long-Lasting:

One of the primary features of money is that it should be long-lasting. Who would want to have money if it is not durable and perish within a specific period? Nobody! That is the problem of using salt or wheat because eventually, they expire and cannot be stored for a long time without being damaged.

However, some other forms of money used in the old days would last long. Yes, we are talking about precious metals like gold and silver. This is among the reasons why precious metals still have a great deal of popularity among people.

- Divisibility:

If you wanted a bag of wheat and you have a stone to offer in exchange for that (yes! Stones were used at a particular time for exchange), but the bag of wheat is only worth half the stone. How are you going to accomplish what you desired?

Therefore, money should have divisibility, which is especially important to make transactions of an exact value. Like when you buy something worth $2.50 and give $3 to the seller, the seller returns $0.50.

- Convenience:

Imagine that you were in one of those ages mentioned, and you were throwing a massive party to all your friends, relatives, and family members. For this, you need many objects such as fruits, vegetables, meat, wheat, and many other things. Let us assume that, by that time, the only thing that money is was salt. Now let us say that ten bags of salt get you one bag of wheat, and you need ten bags of wheat. How are you going to transport 100 bags of salt? Even if you do so, how could you have stored them?

Nowadays, if you wanted to buy something, you could just pay in cash or even make a card transaction or transfer money online. In such a way, money should be very convenient to use, whether for carrying or storing.

- Constant value:

Money must constantly maintain its value because when it is volatile, people will not continue to have money worth the weight they acquired earlier. Moreover, people will face many difficulties if the money cannot consistently maintain its value.

- Intrinsic Value:

Intrinsic value is nothing but the underlying value of the asset. So, for example, cash worth $100 is not worth $100 as it doesn't have that much value (since it is nothing but paper). However, gold can fulfill this obligation as gold has the underlying value/intrinsic value. This means that $1,000 worth of gold has an actual value of $1,000.

- Rarity:

Money should be rare. If it were available everywhere, it would not have that much value, which means people cannot use it to get what they want.

- Acceptance:

Another significant characteristic of money is that it is accepted anywhere. Unless it is accepted everywhere by everyone, it defeats the primary purpose of being used by people to get what they want.

Depending on these characteristics, precious metals and cryptocurrencies are the only types of money that are considered flawless and an ideal form of money.

Cryptography – Cryptography is the method of making something secure and confidential, which is the most relevant term for information/data. Cryptography is achieved by creating code, which makes the respective data invisible. Why does anybody want some data to be hidden? People generally have some confidential data, which must be made invisible. Otherwise, people who are not authorized to access that data will get their hands on it.

Hence, that very data is made secure with the help of cryptography, which makes it available for the people for whom that data is intended.

The currency that has been made confidential with the help of cryptography is known as cryptocurrency. The most common types of algorithms used for cryptocurrencies are ‘Secret Key Cryptography’, ‘Public Key Cryptography’, and ‘Hash Functions’.

As discussed before, cryptocurrency is a type of digital currency or virtual currency that uses cryptography. So, why is a currency needed to be made secure with the help of cryptography? By doing so, the currency can be made a genuine one without having the possibility of being counterfeited or double-spent.

Most of the cryptocurrencies, if not all of them, run based on a particular type of technology known as ‘Blockchain’. To understand how exactly NFTs and Ethereum work, it is highly recommended that everyone reading this book must know about the concept of blockchain and how that technology works. However, if you already have a general idea about the concept, we still suggest you stay with us to understand some things you might not have heard.

Chapter 7: Crypto Mining

Just so that we can understand the process of crypto mining easily, we will have a quick overview of crypto mining.

- Verification of Transactions by nodes:

Transactions are a crucial aspect when it comes to the composition of a cryptocurrency blockchain network.

- Individual transaction data is entered into a list of other transactions for forming a block in the blockchain:

In crypto mining, all the transaction data is bundled into a particular list and added to a new data block. When the transaction is added to the blockchain (after successful verification of the transaction), you will not be able to double spend the fraction of bitcoin. This is done by adding the transaction data to a permanent and public ledger. No further changes can be made to that specific data after being successfully added to a block.

- Along with some other data, a hash is added to an unconfirmed block:

After there have been enough transactions added to an unconfirmed block, some extra information is added, i.e., the header data, a hash from the previous block, and a new hash for that new block. So, what exactly happens here is that the header data of the previous block and a nonce are combined to create the new hash for the new block. Then, this new hash is added to the new unconfirmed block to be verified by a miner.

This is where you take action, and let us think that you were able to solve that. So now, you send a message to all the other miners present on the blockchain network that the mission was accomplished, and they must verify that.

How sophisticated might a hash be? Let us see an example. When you see “92a113d6d9de32e1012bc479b5225cf30850bef62b5b4855c5a436a56defb8af what exactly comes to your mind? It does not make any sense. But when we decipher it with the help of the SHA256 hash, we can see that the data is “cryptocurrency and blockchain”.

- Other miners verify it to make sure it is legit:

After you have let the other miners on the blockchain network know that you’ve successfully done it, they will have to check whether the unconfirmed block is legit by checking the node.

- After it is confirmed, it gets published on the blockchain:

Now, the PoW is complete, and it calls for a celebration when the new block of data has been confirmed. Even though the PoW consensus takes up a lot of time and effort, this is an efficient way of stating that you have solved the hash and the other miners can verify it. Since the block has been added will be the most recent block, it is added at the end of the blockchain network. In general, all the blocks in the blockchain network are added chronologically and are added next to the previously published blocks.

The transaction data that is being added to the ledger is encrypted using public-key cryptography. To be added to the blockchain, the blocks must make use of a hash that is verified by the miner nodes on that particular blockchain. In this way, unauthorized transactions and modifications to the existing data can be prevented.

As there is no specific authority for overseeing the transactions, the computers used for mining are responsible for the ledger. Generally, the updates being made to the blockchain are frequent, and according to some research, it has been estimated that a new block of data is added every ten minutes with the help of mining when it comes to bitcoin.

Because of the blockchain, any individual can see and update the ledger as it is public. When you are a crypto miner, you will be using your computer

to generate random guesses for solving the cryptographic hash. When we consider fishing, for example, if you are lucky, you will catch a fish. Otherwise, you keep on until you catch one. Similarly, if you are fortunate enough, you will be successful in solving a puzzle and get a reward, and if not, you keep going until you succeed. After trying a lot, most people would generally drop the mining process and opt for other ways of earning money.

Why would anybody mine? – We have seen that the chances of successfully solving the hash function and getting a reward for that depend on sheer luck. So, why would anybody want to go ahead and waste their precious time, effort, and money (for buying and maintaining the necessary equipment) if the chances of getting rewarded are based on luck?

There are many cryptocurrencies in existence, which most of you might not be familiar with. Most of you may have heard Bitcoin, Ethereum, Dash, but there are several thousands of cryptocurrencies in existence in real-time. By the time of writing this book, there are more than 4,500 cryptocurrencies in existence. Cryptocurrencies involve volatility, and the value of these cryptocurrencies experiences fluctuations daily.

As time passes, more and more people are attracted to making transactions online using digital money instead of standard money.

People are starting to have a little bit of doubt about the existing monetary systems. Most people would like to have control over their money and maintain discretion while managing their finances. The general ideology is that the government does not need to know what you purchase or how much you spend on your needs and necessities.

To avoid being under the surveillance of the centralized monetary authorities, some people might opt for hiding money under their basements or in an old dusty mattress in their attic (just kidding). However, there is an efficient way people can discretely use their money without involving the traditional centralized banking authorities. This can be achieved with the help of mining and making use of cryptocurrencies. Most cryptocurrencies offer a maximum level of anonymity to the people for using their money. Because of this, the implementation of the crypto mining process uses public-key encryption and hash functions.

People who mine cryptocurrencies are paid a small amount of those cryptocurrencies as a reward for their effort. This is usually a profitable aspect, yet we must consider that most people might not get the returns over the money spent by them for the resources. When a cryptocurrency is rare in nature, like bitcoin, the miners will benefit from the rewards they receive.

Cryptocurrencies are new and are gaining popularity all over the world. As a result, there has been a significant increase in the number of people who trade with them, store them, use them, and mine them.

Types of mining – As we have understood what crypto mining is, now we will see some of the types of crypto mining.

- Cloud Mining:

Cloud Mining is one of the most common ways of mining cryptocurrencies, which does not require much effort. However, it is a process where you will be required to pay a specific amount of money and rent out their mining equipment called a ‘mining rig’, along with mining itself. In most cases, such types of mining rigs are made available by giant corporations.

This rental period would be up to a specific time that has been agreed upon by both parties. All the earnings obtained from these mining rigs would be provided to you while excluding the electricity and maintenance costs. These profits, which are generally received in the form of a cryptocurrency, would be transferred to your crypto wallet.

As mentioned above, mining facilities are offered these rigs, consisting of hundreds of mining rigs that operate together. As they are maintaining such colossal mining rigs, they have a complete idea about what they are doing, and subsequently, they are familiar with the process of mining.

Cloud mining is highly advantageous to the people who do not want to set up their mining rig or can’t afford one. Cloud mining is further classified into two different categories, which are free and paid. Generally, people tend to be attracted to the free mining process, but you should consider that it has its

own set of potential drawbacks. For example, the mining speed is comparatively low, and some additional terms & conditions are involved with this.

However, paid mining is somewhat beneficial in the cloud mining process. All you must do is search for a good cloud mining host online, select one of their best plans that is suitable for you. Generally, these hosts offer 3 or 4 types of paid plans based on the features, and some might even allow you to customize your cloud mining paid plan. These sorts of plans might vary between $500 to $5,000 depending on the method chosen. Then, you must pay the amount mentioned in the plan and register your crypto wallet code with them. It is estimated that most people get the amount invested within six months to one year and profit from there. However, it would be best if you did not forget that cryptocurrencies are volatile, and nobody can anticipate a price drop.

- CPU Mining:

The name itself tells everything you need to know about this type of mining process. Processors are used in this mining process for mining cryptocurrencies, yet this is not considered beneficial.

Simple? Yes, definitely. Effective? We do not think so. Compared to other types of mining, CPU mining is extremely slow, and people might be required to wait for a longer time without having any potential returns. In most cases, people do not even get 10% of their electricity and cooling process spending. You can benefit from this process if you have meager electricity costs and excellent cooling for your processors.

So, why would anyone want to go ahead with such a mining process if it is not beneficial to them? That is because any person having a computer, especially a desktop, can start this type of mining. Yes, it can also be done on laptop computers, but laptops cannot sustain the heat, and all the circuits in a laptop would be fried in a few hours after starting the mining process. People who want to mine cryptocurrencies while not having enough knowledge on the topic proceed with this mining, do it for a few days, and stop after knowing they will not be getting money.

- GPU Mining:

The first thing that comes into mind for most people when talking about cryptocurrency mining is ‘GPU Mining’. One of the widely practiced mining processes and GPU rigs are the things that pop right into the mind while talking about cryptocurrency mining.

GPU rigs are the mining rigs that are even used in the cloud mining process as well. So, if you are doing it as an individual, it will be called GPU Mining, but if an extensive mining facility with hundreds of mining rigs does it, it would be called cloud mining.

Even though the costs involved with the construction of a GPU mining rig are costly, the efficiency of the hash speed and general workforce is excellent. Building a GPU mining from scratch would cost around $3,000, but the person will get profits much faster than he/she can get from CPU mining. A GPU rig usually consists of a processor, motherboard, cooling system, frame, and graphic cards. Graphic cards are the essential components in the GPU mining process for mining cryptocurrencies.

- ASIC Mining:

Application-Specific Integrated Circuits (ASICs) are unique devices with an only primary objective of mining cryptocurrencies. Compared to other types of methods such as CPU Mining and GPU Mining, ASICs are highly advanced and highly effective in producing cryptocurrencies.

So, why are we even being bothered by talking about CPU Mining, GPU Mining when ASIC Mining is an extremely efficient way of mining cryptocurrencies? There is a reason for that, i.e., the controversy related to it. As ASICs are the most powerful, the chances of earning rewards with the help of GPU mining and CPU mining will become lesser. Therefore, so many miners started to protest ASIC mining to still have a chance by using GPU mining and CPU mining.

Therefore, if you choose to become a miner, it is better to opt for GPU mining or cloud mining.

Why isn't everyone doing it? - Even though there has been a considerable increase in the number of people who mine cryptocurrencies, the increase is not that large. Why is that so, and what are the reasons that people still aren't wholly getting involved in the process of mining and become miners? There are several reasons for that, and we will look at some of the significant drawbacks of cryptocurrency mining.

- As discussed, crypto mining requires a significant amount of money to start a rig because you would have to buy the equipment and manage the costs related to it, such as electricity and other maintenance costs.

- Along with that, you will need a lot of computing power to be the first person to solve the hash functions.

- The reward goes on decreasing as time goes on. For instance, if we consider bitcoin, the compensation earned by miners used to be 50 BTC at the beginning (2009). But as of now, the reward has been reduced to 6.25 BTC. In this way, every five years, the compensation offered to miners for solving the cryptographic hash function gets reduced by half.

- Not only does the reward gets reduced, but the complexity of the cryptographic function also becomes tougher with time. This would generally result in the requirement of higher computing power, which would require more money to be put into the process to maintain the mining rig.

- Finally, some governments do not approve of their citizens getting connected with any activity related to cryptocurrencies. Therefore, if you are from such a country, then there will be a possibility that you cannot start a mining rig in your country or get involved with such activities.

- There might even be taxation on the profits earned from crypto

mining depending on the geographical location you are starting a mining rig.

Having discussed that, let us have a brief yet detailed rundown on the advantages and disadvantages of crypto mining.

Advantages – First of all, we will look at the benefits of crypto mining.

- Money:

Yes, the most crucial advantage of mining cryptocurrencies is that you would be able to get money.

- Reduction in the difficulty:

We said that the complexity of solving the hash functions becomes more challenging with time. We noted that for a reason, and we will discuss it in a few moments.

However, from the end of 2018, bitcoin's mining difficulty has dropped by 15%, which is the second-largest drop in the difficulty level so far. The first significant drop being 18% in the year 2011.

The drop in the difficulty is because many bitcoin miners stopped their mining rigs after the crash of cryptocurrencies in the prior months.

When the number of miners on a blockchain experiences a decrease, the complexity of solving the hash functions also decreases with it.

We said that the difficulty level is getting increased with time, yet we again noted that there had been a drop in the difficulty level. Why is that? Let us take the blockchain network of Bitcoin, for example. Here, bitcoin's blockchain network works so that a block of data will be added to the blockchain every ten minutes on average. Which roughly leads to adding 2,016 blocks of data every week.

When the number of miners in a blockchain network decreases, the

computing power is also reduced. The blockchain adjusts itself so that for every week, when there is higher computing power in use, the complexity increases, and simultaneously when the computing power is reduced, the complexity also decreases. So, if you start a mining rig when there are many mining rigs in existence, you might require higher computing power and vice versa.

- Cloud mining:

We have already discussed that cloud mining is rapidly gaining attention among people. There are two reasons for this: cost efficiency and a lesser requirement for time and effort.

When a person opts for setting up his/her mining rig, plenty of money must be spent on the hardware equipment and electricity, which could be avoided entirely with the help of cloud mining. The process for that is also straightforward. You create an account with the cloud mining host, select your requirements, and pay the amount. Simple as that.

- Resale:

If you do not like to acquire the services offered by cloud mining facilities, you can go for your individual mining rig. Meaning you would have to buy your equipment, manage the maintenance. On the bright side, even if you wanted to stop being a miner or if anything happened to cryptocurrencies all over the world, then you would still be having the equipment. This equipment can be sold again for at least the money that has been spent on acquiring it—half glass full mindset.

- Contribution:

By becoming a miner, you would be playing a significant role in the development of cryptocurrencies and becoming one of the contributing members of the cryptocurrency community. If a cryptocurrency has been accepted worldwide instead of centralized money, you will be a person that

has contributed to its success. Making the world a better place for your future generations, you get what we are saying?

Disadvantages – Those are some of the advantages of cryptocurrency mining. Now, let us look at the half glass empty side, meaning the disadvantages.

- Lack of awareness:

There is no denying that cryptocurrencies happen to be highly sophisticated, and the very concept of it is still a mystery to most people in the world. “It’s rocket science! it’s quantum physics! No! it’s a cryptocurrency”. As hard as it might sound to be true, this is the fact. Most people are not even familiar with cryptocurrency (let alone its mining process).

Let us say that you are a college student and asked a thousand dollars from your friend or family member for joining the cloud mining pool. Even if trying to make them understand what you are saying, most people would still not be interested in such types of ventures as they have truly little knowledge of the concept.

- Complex:

It is not easy to start mining as there would be a requirement for the hardware, electricity, cooling equipment, place to fix all these. So, if we have not described everything in detail, what would be your reaction when you hear the words such as GPU mining, ASIC, cloud mining pool? It would sound a bit hard to understand these aspects, right?

Even after knowing about all these aspects, you would still need a lot of time and effort and no need to say money.

- Costs:

First, you would need to buy hardware such as processors if you are

willing to set up an individual mining rig. For that, you need money. Now, this equipment will not run on its own, right? You need electricity for that. Again. Money! So, these processors and other hardware must work very efficiently to solve a complex hash function, and such types of equipment get heated quickly. To cool these, you will need equipment related to cooling, and what will you need again? Exactly!

Moreover, if you do not have your place to set up a mining rig, you would have to rent it. You are using hardware equipment, which means that you will be facing technical issues and other relevant problems every now and then. To rectify such issues, you know what is necessary. You can see where we are going with this.

- Increase in the difficulty:

We already discussed that reducing the number of miners on a blockchain network would reduce the difficulty level. Similarly, when there is an increase in the number of miner nodes present in a blockchain network, there will be an increased difficulty level.

- Illegal Activities:

People who opt for cloud mining companies are usually at the risk of being vulnerable to a scam. Many fake companies and illegal organizers want to make you pay the subscription plan amount along with your mined coins while you remain with a bit of amount, which is not all a reasonable thing for your efforts. If you want to go with cloud mining, it is suggested that you do some ground research and make sure that you choose a renowned company with good feedback from the public.

- Possibility of loss:

We are being optimistic and stating that you would generally get rewards from your mining process after a certain period. However, you should not take it for granted because there is a possibility that you might even lose the

money. If we look at the last few years, we have learned that cryptocurrency prices are highly volatile. Therefore, there is a possibility of prices going down drastically while affecting the mining rig's profits. Also, based on the costs related to the hardware, electricity, and cooling, a decrease in the prices could mean that you are spending more money on the mining rig when compared to the cryptocurrency you're receiving back in tokens. Therefore, using an ASIC miner can be highly beneficial, yet you might have to be on the lookout for the downsides of using an ASIC miner, as we have discussed before.

Final Word:

NFTs allow people to have many things under their own while being present on a decentralized blockchain. Based on all the features and advantages that we have discussed, NFTs may become the next best thing and could get as much hype as Bitcoin did in the past. However, they have a few disadvantages, and we hope they would overcome those shortly.

Based on the information provided in this book, you can choose whether you would like to get involved (buy, sell, or create) with NFTs. Sure, they can be the gateway to a new future, yet there is a controversial discussion about cryptos in many countries.

We hope that this book came in handy for you in knowing all the aspects revolving around Cryptocurrencies, Blockchain, Ethereum, and especially NFTs. Thanks for reading.

For a full beginners guide on Bitcoin and Cryptocurrencies check out my other book: **Bitcoin Gold: Beginners Guide To Bitcoin And Cryptocurrency (ISBN: 979-8717551847) (ASIN: B08Y5KRV94)**